Information in the US-CERT Cyber Security Bulletin is a compilation and includes information published by outside sources, so the information should not be considered the result of US-CERT analysis. Software vulnerabilities are categorized in the appropriate section reflecting the operating system on which the vulnerability was reported; however, this does not mean that the vulnerability only affects the operating system reported since this information is obtained from open-source information.

This bulletin provides a summary of new or updated vulnerabilities, exploits, trends, viruses, and trojans. **Updates to vulnerabilities that appeared in previous bulletins are listed in bold text.** The text in the Risk column appears in red for vulnerabilities ranking High. The risks levels applied to vulnerabilities in the Cyber Security Bulletin are based on how the "system" may be impacted. The Recent Exploit/Technique table contains a "Workaround or Patch Available" column that indicates whether a workaround or patch has been published for the vulnerability which the script exploits.

Vulnerabilities

- Windows Operating Systems
  - Adobe Acrobat and Reader File Discovery
  - **Adobe Acrobat Reader Invalid-ID-Handle-Error Remote Code Execution (Updated)**
  - Altiris Deployment Solution AClient Security Bypass
  - BulletProof FTP Server Privilege Escalation
  - Cybration ICUII Password Disclosure
  - Ecomm Professional Guestbook "AdminPWD" SQL Injection
  - enVivo!soft enVivo!CMS SQL Injection and Privilege Escalation
  - ExoticSoft FilePocket Password Disclosure
  - GlobalSCAPE Secure FTP Server Buffer Overflow Lets Remote Users Execute Arbitrary Code
  - **Intersoft NetTerm Remote Code Execution (Updated)**
  - Kerio Products Password Brute Force and Denial of Service
  - MaxWebPortal SQL Injection and Privilege Escalation
  - Metalinks MetaBid Three SQL Injection Vulnerabilities
  - NetLeaf Limited NotJustBrowsing Discloses Application Passwords
  - Ocean12 Mailing List Manager Remote SQL Injection
  - Raysoft Video Cam Server Multiple Vulnerabilities
  - Skype for Windows Security Bypass
  - soft3304 04WebServer Directory Traversal
  - Software602 602LAN SUITE Local File Detection and Denial of Service
  - StorePortal Multiple SQL Injection High
  - StumbleInside GoText Discloses Users Configuration Data
  - Symantec AntiVirus Products RAR Archive Virus Detection Bypass
  - Uapplication Products Password Disclosure
  - WWWguestbook SQL Injection
- UNIX / Linux Operating Systems
  - Apple Mac OS X Default Pseudo-Terminal Permission
  - Apple Safari Web Browser HTTPS Denial of Service
  - APSIS Pound Remote Buffer Overflow
  - **Carnegie Mellon University Cyrus IMAP Server Multiple Remote Buffer Overflows (Updated)**
  - Cocktail Admin Password Disclosure
  - Debian CVS-Repouid Remote Authentication Bypass & Denial of Service
  - ESRI ArcInfo Workstation s Buffer Overflows and Format String
  - **GNU Sharutils Multiple Buffer Overflow (Updated)**
  - **GNU Sharutils 'Unshar' Insecure Temporary File Creation (Updated)**
  - **GNU Lysator LSH Remote Denial of Service (Updated)**
  - GnuTLS Padding Validation Remote Denial of Service
  - HP OpenView Event Correlation Services
  - HP OpenView Network Node Manager
  - **Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow (Updated)**
  - Joshua Chamas Crypt::SSLeay Perl Module Insecure Entropy Source
  - **ProZilla Initial Server Response Format String (Updated)**
  - **KDE Kommander Remote Arbitrary Code Execution (Updated)**
  - **LBL TCPDump Remote Denials of Service (Updated)**
  - Linux Kernel it87 & via686a Drivers Denial of Service
  - MandrakeSoft LAM/MPI Runtime Insecure Account Creation
  - Marc Lehmann Convert-UUlib Perl Module Buffer Overflow
  - Mtp Target Format String and Denial of Service
  - **Multiple Vendors ImageMagick Remote Buffer Overflow (Updated)**
  - **Multiple Vendors KDE 'kimgio' image library Remote Buffer Overflow (Updated)**
  - **Multiple Vendors Perl 'rmtree()' Function Elevated Privileges (Updated)**
  - **Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities (Updated)**
  - **Multiple Vendors Perl File::Path::rmtree() Permission Modification Vulnerability (Updated)**
  - **Multiple Vendors Squid Proxy Set-Cookie Headers Information Disclosure (Updated)**
  - **Multiple Vendors CVS Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Perl SuidPerl Multiple Vulnerabilities (Updated)**
  - **Multiple Vendors Linux Kernel Bluetooth Signed Buffer Index (Updated)**
  - Multiple Vendors Linux Kernel Itanium System Call Denial of Service
  - **Multiple Vendors Linux Kernel Local Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel PPP Driver Remote Denial of Service (Updated)**
  - **Multiple Vendors Linux Kernel Multiple Vulnerabilities (Updated)**

- **Multiple Vendors Linux Kernel EXT2 File System Information Leak (Updated)**
- **Multiple Vendors Linux Kernel Unw_Unwind_To_User Denial of Service (Updated)**
- **Multiple Vendors Linux Kernel SYS_EPoll_Wait Elevated Privileges (Updated)**
- **Multiple Vendors Gaim Jabber File Request Remote Denial of Service (Updated)**
- **Multiple Vendors Gaim 'Gaim_Markup_Strip_HTML()' Function Remote Denial of Service (Updated)**
- Multiple Vendors Squid Proxy Remote Cache Poisoning
- Multiple Vendors Squid Proxy HTTP Response Splitting Remote Cache Poisoning
- **Multiple Vendors LibXPM Bitmap_unit Integer Overflow (Updated)**
- **Multiple Vendors XLI Internal Buffer Management (Updated)**
- **Multiple Vendors XLoadImage Compressed Image Remote Command (Updated)**
- Nokia Affix Bluetooth Protocol Stack Elevated Privileges
- **Novell Evolution Remote Denial of Service (Updated)**
- Open WebMail Input Validation
- osTicket Multiple Vulnerabilities
- **PHP Group Exif Module IFD Tag Integer Overflow (Updated)**
- PHPMyAdmin Insecure SQL Install Script
- PostgreSQL Remote Denial of Service & Arbitrary Code Execution
- **Postgrey Format String (Updated)**
- **Red Hat BCM5820 Linux Driver Buffer Overflow (Updated)**
- RedHat Enterprise Linux Native POSIX Threading Library
- **Rob Flynn Gaim Multiple Remote Denials of Service (Updated)**
- Robert Styma Consulting ARPUS/Ce Buffer Overflow & Race Condition
- Rootkit Hunter Insecure Temporary File Creation
- Survivor Cross-Site Scripting
- **SNMPPD SNMP Proxy Daemon Remote Format String (Updated)**

- Multiple Operating Systems
  - BakBone NetVault 'NVStatsMngr.EXE' Elevated Privileges
  - BEA WebLogic Server & WebLogic Express Cross-Site Scripting
  - Claroline Multiple Vulnerabilities
  - codetosell ViArt Shop Enterprise Cross-Site Scripting
  - Dream4 Koobi CMS Index.PHP P Parameter SQL Injection
  - **Ethereal Etheric/GPRS-LLC/IAPP/JXTA/sFlow Dissector Vulnerabilities (Updated)**
  - GrayCMS Error.PHP Remote Code Execution
  - HP OpenView Radia Management Portal Remote Command Execution
  - **Horde Kronolith Module Parent Frame Page Title Cross-Site Scripting (Updated)**
  - **Horde Passwd Module Parent Frame Page Title Cross-Site Scripting (Updated)**
  - **Horde Turba Module Parent Frame Page Title Cross-Site Scripting (Updated)**
  - **Horde Accounts Module Parent Frame Page Title Cross-Site Scripting (Updated)**
  - **Horde Chora Parent Frame Page Title Cross-Site Scripting (Updated)**
  - **Horde Forwards Module Parent Frame Page Title Cross-Site Scripting (Updated)**
  - **Horde IMP Webmail Client Parent Frame Page Title Cross-Site Scripting (Updated)**
  - **Horde Mnemo Parent Frame Page Title Cross-Site Scripting (Updated)**
  - **Horde Vacation Parent Frame Page Title Cross-Site Scripting (Updated)**
  - **Horde Nag Parent Frame Page Title Cross-Site Scripting (Updated)**
  - Lotus Domino '@SetHTTPHeader' Function HTTP Response Splitting
  - Lotus Domino NRPC Protocol Format String
  - IBM Lotus Notes 'notes.ini' File Denial of Service
  - Invision Power Board Remote Cross-Site Scripting
  - JustWilliam's Amazon Webstore Cross-Site Scripting
  - Morgan Harvey SitePanel Multiple Vulnerabilities
  - **Mozilla Browser and Mozilla Firefox Remote Window Hijacking (Updated)**
  - **Mozilla Suite / Firefox Multiple Vulnerabilities (Updated)**
  - **Mozilla Suite/ Firefox Drag and Drop Arbitrary Code Execution (Updated)**
  - **Mozilla Firefox, Mozilla, and Thunderbird Multiple Vulnerabilities (Updated)**
  - **Mozilla Firefox Image Javascript URI Dragging Cross-Site Scripting Vulnerability (Updated)**
  - **Mozilla Firefox Multiple Vulnerabilities (Updated)**
  - **Mozilla Suite/Firefox JavaScript Lambda Information Disclosure (Updated)**
  - **Multiple Vendors Telnet Client 'slc_add_reply()' & 'env_opt_add()' Buffer Overflows (Updated)**
  - **MPlayer RTSP and MMST Streams Buffer Overflow (Updated)**
  - **Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service (Updated)**
  - **Multiple Vendors Squid Proxy Aborted Connection Remote Denial of Service (Updated)**
  - MyPHP Forum Sender Spoofing
  - Oracle Web Cache / Application Server Vulnerabilities
  - phpBB Notes Mod 'posting_notes.php' Input Validation
  - **PHP cURL Open_Basedir Restriction Bypass (Updated)**
  - **PHP 'getimagesize()' Multiple Denials of Service (Updated)**
  - PHP-Calendar Search.PHP SQL Injection
  - PHPCart Input Validation
  - phpCOIN Multiple SQL Injection
  - Serendipity Multiple Vulnerabilities

Recent Exploit Scripts/Techniques

Trends
Viruses/Trojans

Vulnerabilities

The table below summarizes vulnerabilities that have been identified, even if they are not being exploited. Complete details about patches or workarounds are available from the source of the information or from the URL provided in the section. CVE numbers are listed where applicable. Vulnerabilities that affect **both** Windows and Unix Operating Systems are included in the Multiple Operating Systems section.

Note: All the information included in the following tables has been discussed in newsgroups and on web sites.

The Risk levels defined below are based on how the system may be impacted:

- **High** - A high-risk vulnerability is defined as one that will allow an intruder to immediately gain privileged access (e.g., sysadmin or root) to the system or allow an intruder to execute code or alter arbitrary system files. An example of a high-risk vulnerability is one that allows an unauthorized user to send a sequence of instructions to a machine and the machine responds with a command prompt with administrator privileges.
- **Medium** - A medium-risk vulnerability is defined as one that will allow an intruder immediate access to a system with less than privileged access. Such vulnerability will allow the intruder the opportunity to continue the attempt to gain privileged access. An example of medium-risk vulnerability is a server configuration error that allows an intruder to capture the password file.
- **Low** - A low-risk vulnerability is defined as one that will provide information to an intruder that could lead to further compromise attempts or a Denial of Service (DoS) attack. It should be noted that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered to be a "High" threat.

Windows Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Adobe Adobe Reader 7.0 and earlier Adobe Acrobat 7.0 and earlier	The Acrobat web control in Adobe Acrobat and Acrobat Reader 7.0 and earlier, when used with Internet Explorer, allows remote malicious users to determine the existence of arbitrary files via the LoadFile ActiveX method. This is a separate issue from CAN-2005-1347. Updates available: http://www.adobe.com/support/techdocs/331465.html Currently we are not aware of any exploits for this vulnerability.	Adobe Acrobat and Reader File Discovery CAN-2005-0035	Low	Adobe Advisory, Document 331465, April 1, 2005
Adobe Acrobat Reader 6.0 and prior	A vulnerability has been reported that could let a remote malicious user execute arbitrary code. If a specially crafted PDF file is loaded by Acrobat Reader it will trigger an Invalid-ID-Handle-Error in 'AcroRd32.exe'. No workaround or patch available at time of publishing. **The vendor has been unable to reproduce this vulnerability. The original vulnerability reporter has refused to provide sufficient details to confirm the issue to either Security Tracker or the vendor. This is a separate issue from CAN-2005-0035.** Currently we are not aware of any exploits for this vulnerability.	Adobe Acrobat Reader Invalid-ID-Handle-Error Remote Code Execution **CAN-2005-1347**	High	Security Tracker Alert, 1013774, April 21, 2005, **Updated May 2, 2005**
Altiris Altiris Client Service for Windows version 6.1.393	A vulnerability has been reported that could let local malicious users bypass certain security restrictions. This is due to an error in ACLIENT.EXE that lets a user bypass the password restriction and gain access to the "Altiris Client Service Properties" window without supplying a valid password. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Altiris Deployment Solution AClient Security Bypass	Medium	Security Focus, Bugtraq ID 13409, April 29, 2005
BulletProof Software BulletProof FTP 2.4.0.31	A vulnerability has been reported that could let local malicious users gain escalated privileges. This is due to the application invoking the help functionality with SYSTEM privileges when configured to run as a service. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	BulletProof FTP Server Privilege Escalation CAN-2005-1371	Medium	Secunia Advisory, SA15152, April 28, 2005
Cybration ICUII 7.0	A vulnerability has been reported that could let a local malicious user obtain passwords. This is because the application password and instant messenger application passwords are stored in plain text format. The file may contain MSN, Yahoo, AIM, and ICQ user passwords. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Cybration ICUII Password Disclosure CAN-2005-1411	Medium	Security Focus Bugtraq ID: 13441, April 29, 2005

Ecommerce-Carts.com Ecomm Professional Guestbook 3.x	An input validation vulnerability has been reported that could let a remote malicious user conduct SQL injection attacks. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Ecomm Professional Guestbook "AdminPWD" SQL Injection CAN-2005-1412	High	Secunia Advisory, SA15190, April 29, 2005
enVivo!soft enVivo!CMS	A vulnerability has been reported that could let a remote malicious user inject SQL commands to gain access to the application. The 'admin_login.asp' script does not properly validate user-supplied input in the 'username' and 'password' parameters. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	enVivo!soft enVivo!CMS SQL Injection and Privilege Escalation CAN-2005-1413	High	Dcrab 's Security Advisory, April 29, 2005
ExoticSoft FilePocket 1.2	A vulnerability has been reported that could let a local malicious user view passwords. Proxy passwords are stored in the Windows registry in plain text format. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	ExoticSoft FilePocket Password Disclosure CAN-2005-1414	Medium	Security Tracker Alert, 1013823, April 28, 2005
GlobalSCAPE Secure FTP Server 3.0.2	A buffer overflow vulnerability has been reported that could let a remote malicious user execute arbitrary code on the target system. The remote user can overwrite the EIP (and SEH) registers with an arbitrary address. The vendor has reportedly issued a fix: http://www.cuteftp.com/gsftps/ Proofs of Concept exploit scripts have been published.	GlobalSCAPE Secure FTP Server Buffer Overflow Lets Remote Users Execute Arbitrary Code CAN-2005-1415	High	Security Focus Bugtraq ID 13454, May 2, 2005
Intersoft International NetTerm 4.x, 5.x	A vulnerability has been reported that could let local malicious users execute arbitrary code. This is due to a boundary error in the NetFtpd program which can cause a buffer overflow by passing an overly long argument to the "USER" FTP command when logging in. The vendor has removed NetFtpd in NetTerm 5.1.1.1 and later. Currently we are not aware of any exploits for this vulnerability.	Intersoft NetTerm Remote Code Execution CAN-2005-1323 **Misclassified as Multiple OS in SB05-117.**	High	Secunia Advisory, SA15140 April 27, 2005
Kerio Kerio WinRoute Firewall 6.0.10 and prior Kerio MailServer 6.0.8 and prior Kerio Personal Firewall 4.1.2 and prior	Two vulnerabilities have been reported that could let local users cause a Denial of Service and brute force passwords. Local users can exploit an error in the remote administration protocol to brute force passwords if the username is known. Local users can also exploit an error in the remote administration protocol to consume a large amount of CPU resources by continuously sending messages. The following versions are fixed: * Kerio WinRoute Firewall version 6.0.11 and later. * Kerio MailServer version 6.0.9 and later. * Kerio Personal Firewall version 4.1.3 and later. Currently we are not aware of any exploits for these vulnerabilities.	Kerio Products Password Brute Force and Denial of Service CAN-2005-1062 CAN-2005-1063	Medium	Secure Computer Group Document IDs ID: #20050429-1 and #20050429-2, April 29, 2005
MaxWebPortal MaxWebPortal 1.30 - 1.33	A vulnerability exists that could let a remote malicious user inject SQL commands to gain administrative access. Multiple scripts do not properly validate user-supplied input: article_popular.asp, dl_popular.asp, links_popular.asp, pic_popular.asp, article_rate.asp, dl_rate.asp, links_rate.asp, pic_rates.asp, article_toprated.asp, dl_toprated.asp, links_toprated.asp, pic_toprated.asp. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	MaxWebPortal SQL Injection and Privilege Escalation CAN-2005-1417	High	Security Focus Bugtraq ID 13466, May 2, 2005
Metalinks MetaBid	Multiple vulnerabilities have been reported in MetaBid that could let remote malicious users conduct SQL injection attacks. This is due to input validation errors in the "intAuctionID" parameter in "item.asp" and the username and password fields in "logIn.asp." No workaround or patch available at time of publishing.	Metalinks MetaBid Three SQL Injection Vulnerabilities CAN-2005-1364	High	Dcrab 's Security Advisory, April 27, 2005

	A Proof of Concept exploit has been published.			
NetLeaf Limited NotJustBrowsing 1.0.3	A vulnerability has been reported that could let a local malicious user obtain an application password. This is because the three character 'View Lock Password' is stored in in plain text format. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	NetLeaf Limited NotJustBrowsing Discloses Application Password CAN-2005-1418	Medium	Security Focus, Bugtraq ID 13442, April 29, 2005
Ocean12 Technologies Ocean12 Mailing List Manager 1.06	An input validation vulnerability has been reported that could let a remote malicious user inject SQL commands. Input validation errors exist in the 'Admin_id' and 'Admin_password' fields. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Ocean12 Mailing List Manager Remote SQL Injection CAN-2005-1419	High	Zinho's Security Advisory, April 28, 2005
Raysoft Video Cam Server 1.0.0	Several vulnerabilities have been reported that could let a remote malicious user obtain files from the target system, determine the installation path, and cause a Denial of Service. A remote user can obtain files located outside of the web document directory by supplying a special request, access an administration page to shutdown the camera or the web service, and request a non-existent page to determine the installation path. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Raysoft Video Cam Server Multiple Vulnerabilities CAN-2005-1420 CAN-2005-1421 CAN-2005-1422	Low	Security Tracker Alert, 1013860, May 2, 2005
Skype Skype for Windows 1.2.0.0 to 1.2.0.46	A vulnerability has been reported that could let local malicious users bypass the identity check for an authorized application, then call arbitrary Skype API functions by modifying or replacing that application. Upgrade to Skype for Windows version 1.2.0.47 or higher: http://www.skype.com/download/ Currently we are not aware of any exploits for this vulnerability.	Skype for Windows Security Bypass CAN-2005-1407	Medium	Skype Security Advisory, SSA-2005-01, April 20
soft3304 04WebServer 1.81	A input validation vulnerability has been reported that could let remote malicious users gain knowledge of sensitive information. The contents of files and folders one folder outside the document root could be exposed. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	soft3304 04WebServer Directory Traversal CAN-2005-1416	Low	Secunia Advisory, SA15230, May 3, 2005
Software602 602LAN SUITE 2004.0.05.0413	A vulnerability has been reported that could let remote users detect the presence of local files and cause a Denial of Service. No redirection occurs when accessing the "mail" script with the "A" parameter referencing a valid local file via directory traversal attacks. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Software602 602LAN SUITE Local File Detection and Denial of Service CAN-2005-1423	Low	Secunia Advisory, SA15231, May 3, 2005
StorePortal StorePortal 2.63	Multiple SQL injection vulnerabilities have been reported in the 'default.asp' script, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	StorePortal Multiple SQL Injection CAN-2005-1293	High	Dcrab 's Security Advisory, April 25, 2005
StumbleInside GoText 1.01	A vulnerability has been reported that could let a local malicious user view user configuration data. The software stores user information, including username, e-mail address, and phone number in the 'Program Files\GoText\GoText.bin' file. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	StumbleInside GoText Discloses Users Configuration Data CAN-2005-1424	Low	Security Tracker Alert, 1013825, April 28, 2005

Symantec Web Security 3.x Norton SystemWorks 2005 Norton Internet Security 2005 Norton AntiVirus 2005 Mail Security for SMTP 4.x Mail Security for Exchange 4.x AntiVirus/Filtering for Domino 3.x AntiVirus Scan Engine 4.x	A vulnerability has been reported that could let a remote malicious user bypass certain scanning functionality.This is due to an error in the Symantec Antivirus component when processing encoded or archived content. This can be exploited to crash the decomposer component when parsing a specially crafted RAR file. Updates are available via LiveUpdate and from the vendor: http://www.symantec.com/techsupp/ Currently we are not aware of any exploits for this vulnerability.	Symantec AntiVirus Products RAR Archive Virus Detection Bypass CAN-2005-1346	High	Symantec SYM05-007, April 27, 2005
Uapplication Uguestbook Ublog Reload Uphotogallery	A vulnerability has been reported that could let a remote malicious user obtain the database, which includes the administrative password. A remote authenticated administrator can invoke the uphotogallery 'edit_image.asp' script to upload arbitrary files to the target system. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Uapplication Products Password Disclosure CAN-2005-1425 CAN-2005-1426 CAN-2005-1427 CAN-2005-1428	Medium	Security Tracker Alert, 1013830, April 28, 2005
WWWguestbook 1.1	An input validation vulnerability has been reported that could let a remote malicious user inject SQL commands. The 'login.asp' script does not properly validate input to the 'password' parameter. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	WWWguestbook SQL Injection CAN-2005-1429	High	Security Tracker Alert, 1013837, April 29, 2005

[back to top]

UNIX / Linux Operating Systems Only

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.9, Mac OS X Server 10.0-10.1.5, 10.2-10.2.8, 10.3-10.3.9	A vulnerability has been reported in the pseudo terminal system due to a design error, which could let a malicious user obtain sensitive information. Version 10.4 of Apple Mac OS X reportedly fixes this vulnerability by implementing proper default permissions on the pseudo terminal API. There is no exploit code required.	Apple Mac OS X Default Pseudo-Terminal Permission CAN-2005-1430	Medium	Bugtraq, 397306, May 1, 2005
Apple Safari 1.3	A Denial of Service vulnerability has been reported when processing HTTPS URLs due to insufficient bounds checking. No workaround or patch available at time of publishing. Currently we are not aware of any exploits for this vulnerability.	Apple Safari Web Browser HTTPS Denial of Service CAN-2005-1385	Low	Security Tracker Alert, 1013835, April 29, 2005
APSIS Pound 1.8.2	A buffer overflow vulnerability has been reported in the 'add_port()' function due to a boundary error, which could let a remote malicious user cause a Denial of Service and possibly execute arbitrary code. Upgrade available at: http://www.apsis.ch/pound/Pound-1.8.3.tgz Currently we are not aware of any exploits for this vulnerability.	APSIS Pound Remote Buffer Overflow CAN-2005-1391	Low/ High (High if arbitrary code can be executed)	Security Focus, 13436, April 29, 2005
Carnegie Mellon University Cyrus IMAP Server 2.x	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in mailbox handling due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exists in the imapd annotate extension due to an off-by-one boundary error, which could let a remote malicious user execute arbitrary code; a buffer	Cyrus IMAP Server Multiple Remote Buffer Overflows CAN-2005-0546	High	Secunia Advisory, SA14383, February 24, 2005 Gentoo Linux Security Advisory, GLSA 200502-29, February 23, 2005

	overflow vulnerability exists in 'fetchnews,' which could let a remote malicious user execute arbitrary code; a buffer overflow vulnerability exist because remote administrative users can exploit the backend; and a buffer overflow vulnerability exists in imapd due to a boundary error, which could let a remote malicious user execute arbitrary code. Update available at: http://ftp.andrew.cmu.edu/pub/cyrus/cyrus-imapd-2.2.11.tar.gz Gentoo: http://security.gentoo.org/glsa/glsa-200502-29.xml SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/c/cyrus21-imapd/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Conectiva: ftp://atualizacoes.conectiva.com.br/ ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html OpenPKG: ftp://ftp.openpkg.org/release/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** Currently we are not aware of any exploits for these vulnerabilities.			SUSE Security Announcement, SUSE-SA:2005:009, February 24, 2005 Ubuntu Security Notice USN-87-1, February 28, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:051, March 4, 2005 Conectiva Linux Security Announcement, CLA-2005:937, March 17, 2005 ALTLinux Security Advisory, March 29, 2005 OpenPKG Security Advisory, OpenPKG-SA-2005.005, April 5, 2005 **Fedora Update Notification, FEDORA-2005-339, April 27, 2005**
Cocktail Cocktail 3.5.4	A vulnerability has been reported because the administrator password is passed insecurely, which could let a malicious user obtain sensitive information. No workaround or patch available at time of publishing. There is no exploit code required.	Cocktail Admin Password Disclosure CAN-2005-1387	Medium	Securities, May 1, 2005
Debian CVS 1.11.1 p1	Several vulnerabilities have been reported: a vulnerability was reported because it is possible to bypass the password protection using the pserver access method, which could let a remote malicious user bypass authentication to obtain unauthorized access; and a Denial of Service vulnerability was reported due to an error in Debian's CVS cvs-repouid patch. Debian: http://security.debian.org/pool/updates/main/c/cvs/ Currently we are not aware of any exploits for these vulnerabilities.	Debian CVS-Repouid Remote Authentication Bypass & Denial of Service CAN-2004-1342 CAN-2004-1343	Medium	Debian Security Advisory, DSA 715-1, April 27, 2005
ESRI ArcInfo Workstation on UNIX 9.0	Several vulnerabilities have been reported: a format string vulnerability was reported in the 'lockmgr' and 'wservice' applications, which could let a malicious user execute arbitrary code with root privileges; and a buffer overflow vulnerability was reported in the 'asmaster,' 'asrecovery,' 'asuser,' 'asutulity,' and 'se' applications due to command line argument boundary errors, which could let a malicious user execute arbitrary code with root privileges. Patch available at: http://support.esri.com/index.cfm?fa=downloads.patchesServicePacks.viewPatch&PID=14&MetaID=1015 Proof of Concept exploits have been published. An exploit script has also been published for the format string vulnerability.	ESRI ArcInfo Workstation s Buffer Overflows and Format String CAN-2005-1393 CAN-2005-1394	High	Secunia Advisory, SA15196, May 2, 2005

GNU sharutils 4.2, 4.2.1	Multiple buffer overflow vulnerabilities exists due to a failure to verify the length of user-supplied strings prior to copying them into finite process buffers, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200410-01.xml FedoraLegacy: http://download.fedoralegacy.org/fedora/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sharutils/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ OpenPKG: ftp://ftp.openpkg.org/release Mandrake: http://www.mandrakesecure.net/en/ftp.php **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-377.html** **Trustix:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** We are not aware of any exploits for these vulnerabilities.	GNU Sharutils Multiple Buffer Overflow CAN-2004-1773	Low/ High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory, GLSA 200410-01, October 1, 2004 Fedora Legacy Update Advisory, FLSA:2155, March 24, 2005 Ubuntu Security Notice, USN-102-1 March 29, 2005 Fedora Update Notifications, FEDORA-2005-280 & 281, April 1, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:067, April 7, 2005 **RedHat Security Advisory, RHSA-2005:377-07, April 26, 2005** **Turbolinux Security Advisory, TLSA-2005-54, April 28, 2005**
GNU sharutils 4.2, 4.2.1	A vulnerability has been reported in the 'unshar' utility due to the insecure creation of temporary files, which could let a malicious user create/overwrite arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/sharutils/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-06.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-377.html** **Trustix:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** There is no exploit code required.	GNU Sharutils 'Unshar' Insecure Temporary File Creation CAN-2005-0990	Medium	Ubuntu Security Notice, USN-104-1, April 4, 2005 Gentoo Linux Security Advisory, GLSA 200504-06, April 6, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:067, April 7, 2005 Fedora Update Notification, FEDORA-2005-319, April 14, 2005 **RedHat Security Advisory, RHSA-2005:377-07, April 26, 2005** **Turbolinux Security Advisory, TLSA-2005-54, April 28, 2005**
GNU Lysator LSH 1.5-1.5.5, 2.0	A remote Denial of Service vulnerability has been reported due to an unspecified error. Upgrades available at: http://www.lysator.liu.se/~nisse/archive/ Patch available at: ftp://ftp.lysator.liu.se/pub/security/lsh/lsh-2.0-2.0.1.diff.gz **Debian:** **http://security.debian.org/pool/updates/main/l/lsh-utils/** Currently we are not aware of any exploits for this vulnerability.	Lysator LSH Remote Denial of Service CAN-2005-0814	Low	Secunia Advisory, SA14609, March 17, 2005 **Debian Security Advisory, DSA 717-1, April 27, 2005**

GnuTLS GnuTLS 1.2 prior to 1.2.3; 1.0 prior to 1.0.25	A remote Denial of Service vulnerability has been reported due to insufficient validation of padding bytes in 'lib/gnutils_cipher.c.' Updates available at: http://www.gnu.org/software/gnutls/download.html Currently we are not aware of any exploits for this vulnerability.	GnuTLS Padding Validation Remote Denial of Service CAN-2005-1431	Low	Security Tracker Alert, 1013861, May 2, 2005
Hewlett Packard Company OpenView Event Correlation Services 3.32, 3.33	Several vulnerabilities have been reported due to unspecified errors, which could let a malicious user cause a Denial of Service or execute arbitrary code. Patches available at: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBMA01141 Currently we are not aware of any exploits for these vulnerabilities.	HP OpenView Event Correlation Services CAN-2005-1433	Low/ High (High if arbitrary code can be executed)	HP Security Bulletin, HPSBMA01141, May 2, 2005
Hewlett Packard Company OpenView Network Node Manager 6.2, 6.4, 7.01, 7.50	Several vulnerabilities have been reported due to unspecified errors, which could let a malicious user cause a Denial of Service or execute arbitrary code. Patches available at: http://h20000.www2.hp.com/bizsupport/TechSupport/Document.jsp?objectID=PSD_HPSBMA01140 Currently we are not aware of any exploits for these vulnerabilities.	HP OpenView Network Node Manager CAN-2005-1434	Low/ High (High if arbitrary code can be executed)	HP Security Bulletin, HPSBMA01140, May 2, 2005
Info-ZIP Zip 2.3; Avaya CVLAN, Intuity LX, MN100, Modular Messaging (MSS) 1.1, 2.0, Network Routing	A buffer overflow vulnerability exists due to a boundary error when doing recursive compression of directories with 'zip,' which could let a remote malicious user execute arbitrary code. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/z/zip/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200411-16.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php SUSE: ftp://ftp.SUSE.com/pub/SUSE Red Hat: http://rhn.redhat.com/errata/RHSA-2004-634.html Debian: http://www.debian.org/security/2005/dsa-624 TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ Avaya: http://support.avaya.com/elmodocs2/security/ASA-2005-019_RHSA-2004-634.pdf Fedora Legacy: http://download.fedoralegacy.org/redhat/ http://download.fedoralegacy.org/fedora/1/updates/ **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** Currently we are not aware of any exploits for this vulnerability.	Info-ZIP Zip Remote Recursive Directory Compression Buffer Overflow CAN-2004-1010	High	Bugtraq, November 3, 2004 Ubuntu Security Notice, USN-18-1, November 5, 2004 Fedora Update Notification, FEDORA-2004-399 & FEDORA-2004-400, November 8 & 9, 2004 Gentoo Linux Security Advisory, GLSA 200411-16, November 9, 2004 Mandrakelinux Security Update Advisory, MDKSA-2004:141, November 26, 2004 SUSE Security Summary Report, SUSE-SR:2004:003, December 7, 2004 Red Hat Advisory, RHSA-2004:634-08, December 16, 2004 Debian DSA-624-1, January 5, 2005 Turbolinux Security Announcement, 20050131, January 31, 2005 Avaya Security Advisory, ASA-2005-019, January 25, 200 Fedora Legacy Update Advisory, FLSA:2255, February 1, 2005 **Slackware Security Advisory, SSA:2005-121-01, May 2, 2005**

Joshua Chamas Crypt::SSLeay 0.51	A vulnerability has been reported because a file is employed from a world writable location for its fallback entropy source, which could lead to weak cryptographic operations. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/libn/libnet-ssleay-perl/ There is no exploit code required.	Joshua Chamas Crypt::SSLeay Perl Module Insecure Entropy Source CAN-2005-0106	Medium	Ubuntu Security Notice, USN-113-1, May 03, 2005
Kalum Somaratna ProZilla Download Accelerator 1.0 x, 1.3.0-1.3.4, 1.3.5 .2, 1.3.5 .1, 1.3.5-1.3.5.2 1.3.6	A vulnerability exists due to improper implementation of a formatted string function when handling initial server responses, which could let a remote malicious user execute arbitrary code. **Debian:** **http://security.debian.org/pool/updates/main/p/prozilla/p** An exploit script has been published.	ProZilla Initial Server Response Format String CAN-2005-0523	High	Security Focus, 12635, February 23, 2005 **Debian Security Advisory, DSA 719-1, April 28, 2005**
KDE KDE 3.2-3.2.3, 3.3-3.3.2, 3.4, KDE Quanta 3.1	A vulnerability has been reported due to a design error in Kommander, which could let a remote malicious user execute arbitrary code. Patches available at: ftp://ftp.kde.org/pub/kde/security_patches/f Gentoo: http://security.gentoo.org/glsa/glsa-200504-23.xml **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** Currently we are not aware of any exploits for this vulnerability.	KDE Kommander Remote Arbitrary Code Execution CAN-2005-0754	High	KDE Security Advisory, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200504-23, April 22, 200 **Fedora Update Notification FEDORA-2005-345, April 28, 2005**
LBL tcpdump 3.4 a6, 3.4, 3.5, alpha, 3.5.2, 3.6.2, 3.6.3, 3.7-3.7.2, 3.8.1 -3.8.3	Remote Denials of Service vulnerabilities have been reported due to the way tcpdump decodes Border Gateway Protocol (BGP) packets, Label Distribution Protocol (LDP) datagrams, Resource ReSerVation Protocol (RSVP) packets, and Intermediate System to Intermediate System (ISIS) packets. **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** Exploit scripts have been published.	LBL TCPDump Remote Denials of Service CAN-2005-1278 CAN-2005-1279 CAN-2005-1280	Low	Bugtraq, 396932, April 26, 2005 **Fedora Update Notification, FEDORA-2005-351, May 3, 2005**
Linux kernel 2.6.11 .7	A Denial of Service vulnerability has been reported due to the creation of an insecure file by the kernel it87 and via686a drivers. Patch available at: http://kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.8.bz2 There is no exploit code required.	Linux Kernel it87 & via686a Drivers Denial of Service CAN-2005-1369	Low	Secunia Advisory, SA15204, May 2, 2005
MandrakeSoft lam-runtime-7.0.6-2mdk	A vulnerability has been reported in the LAM/MPI Runtime environment due to the creation of an insecure account, which could let a local/remote malicious user obtain unauthorized access. No workaround or patch available at time of publishing. There is no exploit code required.	MandrakeSoft LAM/MPI Runtime Insecure Account Creation CAN-2005-1379	Medium	Bugtraq, 397157, April 28, 2005
Marc Lehmann Convert-UUlib 1.50	A buffer overflow vulnerability has been reported in the Convert::UUlib module for Perl due to a boundary error, which could let a remote malicious user execute arbitrary code. Update available at: http://search.cpan.org/dist/Convert-UUlib/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-26.xml	Convert-UUlib Perl Module Buffer Overflow CAN-2005-1349	High	Gentoo Linux Security Advisory, GLSA 200504-26, April 26, 2005 Secunia Advisory, SA15130, April 27,2 005

	Currently we are not aware of any exploits for this vulnerability.			
mtp-target.org Mtp-Target for Windows 1.2.2 & prior, Mtp-Target for Linux 1.2.2 & prior	Several vulnerabilities have been reported: a format string vulnerability has been reported in the client code when messages from other users are displayed, which could let a remote malicious user execute arbitrary code; and a remote Denial of Service vulnerability has been reported due to a negative integer overflow from the NeL library. No workaround or patch available at time of publishing. A Proof of Concept exploit script has been published.	Mtp Target Format String and Denial of Service CAN-2005-1401 CAN-2005-1402	Low/ High (High if arbitrary code can be executed)	Securiteam, May 2, 2005
Multiple Vendors ImageMagick 6.0-6.0.8, 6.1-6.1.8, 6.2 .0.7, 6.2 .0.4, 6.2, 6.2.1	A buffer overflow vulnerability has been reported due to a failure to properly validate user-supplied string lengths before copying into static process buffers, which could let a remote malicious user cause a Denial of Service. Upgrades available at: http://www.imagemagick.org/script/binary-releases.php **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** A Proof of Concept exploit has been published.	ImageMagick Remote Buffer Overflow CAN-2005-1275	Low	Security Focus, 13351, April 25, 2005 **Fedora Update Notification FEDORA-2005-344, April 28, 2005**
Multiple Vendors KDE 2.0, beta, 2.0.1, 2.1-2.1.2, 2.2-2.2.2, 3.0-3.0.5, 3.1-3.1.5, 3.2-3.2.3, 3.3-3.3.2, 3.4; Novell Linux Desktop 9; SuSE E. Linux 9.1, x86_64, 9.2, x86_64, 9.3, Linux Enterprise Server 9	A buffer overflow vulnerability has been reported in the 'kimgio' image library due to insufficient validation of PCX image data, which could let a remote malicious user cause a Denial of Service or possibly execute arbitrary code. Patches available at: http://bugs.kde.org/attachment.cgi?id=10325&action=view http://bugs.kde.org/attachment.cgi?id=10326&action=view SuSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-22.xml Debian: http://security.debian.org/pool/updates/main/k/kdelibs/ **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** Denial of Service Proofs of Concept exploits have been published.	KDE 'kimgio' image library Remote Buffer Overflow CAN-2005-1046	Low/ High (High if arbitrary code can be executed)	SUSE Security Announcement, SUSE-SA:2005:022, April 11, 2005 Gentoo Linux Security Advisory, GLSA 200504-22, April 22, 2005 Debian Security Advisory, DSA 714-1, April 26, 2005 **Fedora Update Notification, FEDORA-2005-350, May 2, 2005**
Multiple Vendors Larry Wall Perl 5.0 05_003, 5.0 05, 5.0 04_05, 5.0 04_04, 5.0 04, 5.0 03, 5.6, 5.6.1, 5.8, 5.8.1, 5.8.3, 5.8.4 -5, 5.8.4 -4, 5.8.4 -3, 5.8.4 -2.3, 5.8.4 -2, 5.8.4 -1, 5.8.4, 5.8.5, 5.8.6	A vulnerability has been reported in the 'rmtree()' function in the 'File::Path.pm' module when handling directory permissions while cleaning up directories, which could let a malicious user obtain elevated privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/p/perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml Debian: http://security.debian.org/pool/updates/main/p/perl/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this	Perl 'rmtree()' Function Elevated Privileges CAN-2005-0448	Medium	Ubuntu Security Notice, USN-94-1 March 09, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005 Debian Security Advisory, DSA 696-1 , March 22, 2005 Turbolinux Security Advisory, TLSA-2005-45, April 19, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:079, April 29, 2005**

	vulnerability.			
Multiple Vendors Linux kernel 2.4 .0-test1-test12, 2.4-2.4.29, 2.6, 2.6-test1-test11, 2.6.1-2.6.11	Multiple vulnerabilities have been reported in the ISO9660 handling routines, which could let a malicious user execute arbitrary code. Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for these vulnerabilities.	Linux Kernel Multiple ISO9660 Filesystem Handling Vulnerabilities CAN-2005-0815	High	Security Focus, 12837, March 18, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Ubuntu Security Notice, USN-103-1, April 1, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 **Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005**
Multiple Vendors Perl	A race condition vulnerability was reported in the 'File::Path::rmtree()' function. A remote user may be able to obtain potentially sensitive information. A remote user may be able to obtain potentially sensitive information or modify files. The vendor has released Perl version 5.8.4-5 to address this vulnerability. Customers are advised to contact the vendor for information regarding update availability. Debian: http://security.debian.org/pool/updates/main/p/perl/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/perl/ OpenPKG: ftp://ftp.openpkg.org/release/2.1/UPD/perl-5.8.4-2.1.1.src.rpm Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml Mandrake: http://www.mandrakesoft.com/security/advisories?name=MDKSA-2005:031 SUSE: ftp://ftp.suse.com/pub/suse/ Gentoo: http://security.gentoo.org/glsa/glsa-200501-38.xml **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** Currently we are not aware of any exploits for this vulnerability.	Multiple Vendors Perl File::Path::rmtree() Permission Modification Vulnerability CAN-2004-0452	Medium	Ubuntu Security Notice, USN-44-1, December 21, 2004 Debian Security Advisory, DSA 620-1, December 30, 2004 OpenPKG Security Advisory, OpenPKG-SA-2005.001, January 11, 2005 Gentoo Linux Security Advisory, GLSA 200501-38, January 26, 2005 MandrakeSoft Security Advisory, MDKSA-2005:031, February 8, 2005 SUSE Security Summary Report, SUSE-SR:2005:004, February 11, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200501-38:03, March 15, 2005 **Fedora Update Notification, FEDORA-2005-353, May 2, 2005**
Multiple Vendors Squid Web Proxy Cache 2.5 .STABLE9, .STABLE8, .STABLE7	A vulnerability exists when using the Netscape Set-Cookie recommendations for handling cookies in caches due to a race condition, which could let a malicious user obtain sensitive information. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE9-setcookie.patch Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/	Squid Proxy Set-Cookie Headers Information Disclosure CAN-2005-0626	Medium	Secunia Advisory, SA14451, March 3, 2005 Ubuntu Security Notice, USN-93-1 March 08, 2005 Fedora Update Notifications, FEDORA-2005-275 & 276,

	Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** There is no exploit code required.			March 30, 2005 **Conectiva Linux Security Announcement, CLA-2005:948, April 27, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:078, April 29, 2005**
Multiple Vendors Concurrent Versions System (CVS) 1.x;Gentoo Linux; SuSE Linux 8.2, 9.0, 9.1, x86_64, 9.2, x86_64, 9.3, Linux Enterprise Server 9, 8, Open-Enterprise-Server 9.0, School-Server 1.0, SUSE CORE 9 for x86, UnitedLinux 1.0	Multiple vulnerabilities have been reported: a buffer overflow vulnerability was reported due to an unspecified boundary error, which could let a remote malicious user potentially execute arbitrary code; a remote Denial of Service vulnerability was reported due to memory leaks and NULL pointer dereferences; an unspecified error was reported due to an arbitrary free (the impact was not specified), and several errors were reported in the contributed Perl scripts, which could let a remote malicious user execute arbitrary code. Update available at: https://ccvs.cvshome.org/servlets/ProjectDocumentList Gentoo: http://security.gentoo.org/glsa/glsa-200504-16.xml SuSE: ftp://ftp.suse.com/pub/suse/i Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Trustix: http://http.trustix.org/pub/trustix/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/ Peachtree: http://peachtree.burdell.org/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-387.html **OpenBSD:** **http://www.openbsd.org/errata.html#cvs** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** Currently we are not aware of any exploits for these vulnerabilities.	CVS Multiple Vulnerabilities CAN-2005-0753	Low/ High (High if arbitrary code can be executed)	Gentoo Linux Security Advisory, GLSA 200504-16, April 18, 2005 SuSE Security Announcement, SUSE-SA:2005:024, April 18, 2005 Secunia Advisory, SA14976, April 19, 2005 Fedora Update Notification, FEDORA-2005-330, April 20, 2006 Mandriva Linux Security Update Advisory, MDKSA-2005:073, April 21, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0013, April 21, 2005 Gentoo Linux Security Advisory [UPDATE], GLSA 200504-16:02, April 22, 2005 FreeBSD Security Advisory, FreeBSD-SA-05:05, April 22, 2005 Peachtree Linux Security Notice, PLSN-0005, April 22, 2005 RedHat Security Advisory, RHSA-2005:387-06, April 25, 2005 **Turbolinux Security Advisory, TLSA-2005-51, April 28, 2005**
Multiple Vendors Larry Wall Perl 5.8, 5.8.1, 5.8.3, 5.8.4, 5.8.4 -1-5.8.4-5; Ubuntu Linux 4.1 ppc, ia64, ia32	Multiple vulnerabilities exist: a buffer overflow vulnerability exists in the 'PERLIO_DEBUG' SuidPerl environment variable, which could let a malicious user execute arbitrary code; and a vulnerability exists due to an error when handling debug message output, which could let a malicious user corrupt arbitrary files. Ubuntu: http://security.ubuntu.com/ubuntu/pool/universe/p/perl/ Gentoo: http://security.gentoo.org/glsa/glsa-200502-13.xml Mandrake: http://www.mandrakesoft.com/security/	Perl SuidPerl Multiple Vulnerabilities CAN-2005-0155 CAN-2005-0156	Medium/ High (High if arbitrary code can be executed)	Ubuntu Security Notice, USN-72-1, February 2, 2005 MandrakeSoft Security Advisory, MDKSA-2005:031, February 9, 2005 RedHat Security Advisory, RHSA-2005:105-11, February 7, 2005 SGI Security Advisory, 20050202-01-U, February 9, 2005 SUSE Security Summary

	advisories?name=MDKSA-2005:031 RedHat: http://rhn.redhat.com/errata/RHSA-2005-105.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ SUSE: ftp://ftp.suse.com/pub/suse/ Trustix: http://www.trustix.org/errata/2005/0003/ IBM: ftp://aix.software.ibm.com/aix/efixes/security/perl58x.tar.Z **Fedora:** **http://download.fedora.redhat.com/pub/fedora/linux/core/updates/3/** Proofs of Concept exploits have been published.			Report, SUSE-SR:2005:004, February 11, 2005 Gentoo Linux Security Advisory, GLSA 200502-13, February 11, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0003,February 11, 2005 IBM SECURITY ADVISORY, February 28, 2005 **Fedora Update Notification, FEDORA-2005-353, May 2, 2005**
Multiple Vendors Linux kernel 2.4-2.4.29, 2.6 .10, 2.6-2.6.11	A vulnerability has been reported in the 'bluez_sock_create()' function when a negative integer value is submitted, which could let a malicious user execute arbitrary code with root privileges. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.4/testing/patch-2.4.30-rc3.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-283.html** **http://rhn.redhat.com/errata/RHSA-2005-284.html** **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** A Proof of Concept exploit script has been published.	Linux Kernel Bluetooth Signed Buffer Index CAN-2005-0750	High	Security Tracker Alert, 1013567, March 27, 2005 SUSE Security Announcement, SUSE-SA:2005:021, April 4, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 US-CERT VU#685461 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 **RedHat Security Advisories, RHSA-2005:283-15 & RHSA-2005:284-11, April 28, 2005** **Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005**
Multiple Vendors Linux kernel 2.4-2.4.30	A Denial of Service vulnerability has been reported due to a failure to handle system calls that contain missing arguments. RedHat: http://rhn.redhat.com/errata/RHSA-2005-293.html http://rhn.redhat.com/errata/RHSA-2005-284.html Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Itanium System Call Denial of Service CAN-2005-0137	Low	RedHat Security Advisories, RHSA-2005:284-11 & RHSA-2005:293-16, April 22 & 28, 2005

Multiple Vendors Linux Kernel 2.6.10, 2.6 -test1-test11, 2.6-2.6.11	A Denial of Service vulnerability has been reported in the 'load_elf_library' function. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html **Conectiva: ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Local Denial of Service CAN-2005-0749	Low	Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 **Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6 -test1-test11, 2.6, 2.6.1 rc1&rc2, 2.6.1-2.6.8	A remote Denial of Service vulnerability has been reported in the Point-to-Point Protocol (PPP) Driver. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Trustix: http://http.trustix.org/pub/trustix/updates SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html **RedHat: http://rhn.redhat.com/errata/RHSA-2005-283.html** **http://rhn.redhat.com/errata/RHSA-2005-284.html** **Conectiva: ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel PPP Driver Remote Denial of Service CAN-2005-0384	Low	Ubuntu Security Notice, USN-95-1 March 15, 2005 Trustix Secure Linux Security Advisory, TSL-2005-0009, March 21, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 **RedHat Security Advisories, RHSA-2005:283-15 & RHSA-2005:284-11, April 28, 2005** **Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6 -test9-CVS, 2.6-test1- -test11, 2.6, 2.6.1-2.6.11 ; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	Multiple vulnerabilities exist: a vulnerability exists in the 'shmctl' function, which could let a malicious user obtain sensitive information; a Denial of Service vulnerability exists in 'nls_ascii.c' due to the use of incorrect table sizes; a race condition vulnerability exists in the 'setsid()' function; and a vulnerability exists in the OUTS instruction on the AMD64 and Intel EM64T architecture, which could let a malicious user obtain elevated privileges. RedHat: https://rhn.redhat.com/errata/RHSA-2005-092.html	Linux Kernel Multiple Vulnerabilities CAN-2005-0176 CAN-2005-0177 CAN-2005-0178 CAN-2005-0204	Low/ Medium (Low if a DoS)	Ubuntu Security Notice, USN-82-1, February 15, 2005 RedHat Security Advisory, RHSA-2005:092-14, February 18, 2005 SUSE Security Announcement, SUSE-SA:2005:018, March 24, 2005 Fedora Security

	Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1/ Conectiva: ftp://atualizacoes.conectiva.com.br/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Conectiva: ftp://atualizacoes.conectiva.com.br/10/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-283.html** **http://rhn.redhat.com/errata/RHSA-2005-284.html** Currently we are not aware of any exploits for these vulnerabilities.			Update Notification, FEDORA-2005-262, March 28, 2005 Conectiva Linux Security Announcement, CLA-2005:945, March 31, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 **RedHat Security Advisories, RHSA-2005:283-15 & RHSA-2005:284-11, April 28, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6, -test1-test 11, 2.6.1- 2.6.11; RedHat Fedora Core2	A vulnerability has been reported in the EXT2 filesystem handling code, which could let malicious user obtain sensitive information. Patches available at: http://www.kernel.org/pub/linux/kernel/v2.6/patch-2.6.11.6.bz2 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/2/ Trustix: http://http.trustix.org/pub/trustix/updates/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel EXT2 File System Information Leak CAN-2005-0400	Medium	Security Focus, 12932, March 29, 2005 Trustix Secure Linux Security Advisory, TSLSA-2005-0011, April 5, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 **Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005**
Multiple Vendors Linux kernel 2.6.10, 2.6, -test9-CVS, -test1-test11, 2.6.1-2.6.9; RedHat Desktop 4.0, Enterprise Linux WS 4, ES 4, AS 4	A Denial of Service vulnerability has been reported in the 'Unw_Unwind_To_User' function. RedHat; http://rhn.redhat.com/errata/RHSA-2005-366.html http://rhn.redhat.com/errata/RHSA-2005-293.html **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-284.html** Currently we are not aware of any exploits for this vulnerability.	Linux Kernel Unw_Unwind_To_User Denial of Service CAN-2005-0135	Low	RedHat Security Advisory, RHSA-2005:366-19 & RHSA-2005-2935 , April 19 & 22, 2005 **RedHat Security Advisory, RHSA-2005:284-11, April 28, 2005**

Multiple Vendors Linux kernel 2.6-2.6.11	A vulnerability has been reported in 'SYS_EPoll_Wait' due to a failure to properly handle user-supplied size values, which could let a malicious user obtain elevated privileges. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/linux-source-2.6.8.1 Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-366.html **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** An exploit script has been published.	Linux Kernel SYS_EPoll_Wait Elevated Privileges CAN-2005-0736	Medium	Security Focus, 12763, March 8, 2005 Ubuntu Security Notice, USN-95-1 March 15, 2005 Security Focus, 12763, March 22, 2005 Fedora Security Update Notification, FEDORA-2005-262, March 28, 2005 Fedora Update Notification FEDORA-2005-313, April 11, 2005 RedHat Security Advisory, RHSA-2005:366-19, April 19, 2005 **Conectiva Linux Security Announcement, CLA-2005:952, May 2, 2005**
Multiple Vendors RedHat Fedora Core3, Core2; Rob Flynn Gaim 1.2; Peachtree Linux release 1	A remote Denial of Service vulnerability has been reported when an unspecified Jabber file transfer request is handled. Upgrade available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-05.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-365.html Mandrake: http://www.mandrakesecure.net/en/ftp.php SGI: http://www.sgi.com/support/security/ Peachtree: http://peachtree.burdell.org/updates/ **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** There is no exploit code required.	Gaim Jabber File Request Remote Denial of Service CAN-2005-0967	Low	Fedora Update Notifications, FEDORA-2005-298 & 299, April 5, 2005 Gentoo Linux Security Advisory, GLSA 200504-05, April 06, 2005 RedHat Security Advisory, RHSA-2005:365-06, April 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:071, April 14, 2005 SGI Security Advisory, 20050404-01-U, April 20, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 **Conectiva Linux Security Announcement, CLA-2005:949, April 27, 2005**

Multiple Vendors RedHat Fedora Core3, Core2; Rob Flynn Gaim 1.2; Ubuntu Linux 4.1 ppc, ia64, ia32; Peachtree Linux release 1	Two vulnerabilities have been reported: a remote Denial of Service vulnerability has been reported due to a buffer overflow in the 'gaim_markup_strip_html()' function; and a vulnerability has been reported in the IRC protocol plug-in due to insufficient sanitization of the 'irc_msg' data, which could let a remote malicious user execute arbitrary code. Update available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-05.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-365.html Mandrake: http://www.mandrakesecure.net/en/ftp.php SGI: http://www.sgi.com/support/security/ Peachtree: http://peachtree.burdell.org/updates/ **Conectiva: ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for these vulnerabilities.	Gaim 'Gaim_Markup_Strip_HTML()' Function Remote Denial of Service & IRC Protocol Plug-in Arbitrary Code Execution CAN-2005-0965 CAN-2005-0966	Low/ High (High if arbitrary code can be executed)	Fedora Update Notifications, FEDORA-2005 -298 & 299, April 5, 2005 Ubuntu Security Notice, USN-106-1 April 05, 2005 Gentoo Linux Security Advisory, GLSA 200504-05, April 06, 2005 RedHat Security Advisory, RHSA-2005:365-06, April 12, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:071, April 14, 2005 SGI Security Advisory, 20050404-01-U, April 20, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 **Conectiva Linux Security Announcement, CLA-2005:949, April 27, 2005**
Multiple Vendors Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 STABLE5, 2.3 STABLE4, 2.4 STABLE7, 2.4 STABLE6, 2.4, STABLE2, 2.5 STABLE3-STABLE7, 2.5 STABLE1	A vulnerability has been reported when handling upstream HTTP agents, which could let a remote malicious user poison the web proxy cache. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/squid-2.5.STABLE9.tar.gz There is no exploit code required.	Squid Proxy Remote Cache Poisoning CAN-2005-0174	Medium	Squid Proxy Cache Security Update Advisory, SQUID-2005:4, April 23, 2005
Multiple Vendors Squid Web Proxy Cache 2.0 PATCH2, 2.1 PATCH2, 2.3 STABLE5, 2.3 STABLE4, 2.4 STABLE7, 2.4 STABLE6, 2.4, STABLE2, 2.5 STABLE3-STABLE7, 2.5 STABLE1	A vulnerability has been reported due to a failure to handle CR/LF characters in HTTP requests, which could let a remote malicious user poison the web proxy cache. Patches available at: http://www.squid-cache.org/Versions/v2/2.5/squid-2.5.STABLE9.tar.gz There is no exploit code required.	Squid Proxy HTTP Response Splitting Remote Cache Poisoning CAN-2005-0175	Medium	Squid Proxy Cache Security Update Advisory, SQUID-2005:5, April 23, 2005
Multiple Vendors X.org X11R6 6.7.0, 6.8, 6.8.1; XFree86 X11R6 3.3, 3.3.2-3.3.6, 4.0, 4.0.1, 4.0.2 -11, 4.0.3, 4.1.0, 4.1 -12, 4.1 -11, 4.2 .0, 4.2.1 Errata, 4.2.1, 4.3.0.2, 4.3.0.1, 4.3.0	An integer overflow vulnerability exists in 'scan.c' due to insufficient sanity checks on on the 'bitmap_unit' value, which could let a remote malicious user execute arbitrary code. Patch available at: https://bugs.freedesktop.org/attachment.cgi?id=1909 Gentoo: http://security.gentoo.org/glsa/glsa-200503-08.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/l/lesstif1-1/ Gentoo:	LibXPM Bitmap_unit Integer Overflow CAN-2005-0605	High	Security Focus, 12714, March 2, 2005 Gentoo Linux Security Advisory, GLSA 200503-08, March 4, 2005 Ubuntu Security Notice, USN-92-1 March 07, 2005 Gentoo Linux Security Advisory, GLSA 200503-15, March 12, 2005

	http://security.gentoo.org/glsa/glsa-200503-15.xml Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/x/xfree86/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-331.html SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-044.html **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** Currently we are not aware of any exploits for this vulnerability.			Ubuntu Security Notice, USN-97-1 March 16, 2005 ALTLinux Security Advisory, March 29, 2005 Fedora Update Notifications, FEDORA-2005 -272 & 273, March 29, 2005 RedHat Security Advisory, RHSA-2005: 331-06, March 30, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 RedHat Security Advisory, RHSA-2005:044-15, April 6, 2005 **Mandriva Linux Security Update Advisory, MDKSA-2005:080, April 29, 2005**
Multiple Vendors xli 1.14-1.17	A vulnerability exists due to a failure to manage internal buffers securely, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-05.xml Debian: http://security.debian.org/pool/updates/main/x/xli/ ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Mandrake: http://www.mandrakesecure.net/en/ftp.php **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.	XLI Internal Buffer Management CAN-2005-0639	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005 Debian Security Advisory, DSA 695-1, March 21, 2005 ALTLinux Security Advisory, March 29, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:076, April 21, 2005 **SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005**
Multiple Vendors xli 1.14-1.17; xloadimage 3.0, 4.0, 4.1	A vulnerability exists due to a failure to parse compressed images safely, which could let a remote malicious user execute arbitrary code. Gentoo: http://security.gentoo.org/glsa/glsa-200503-05.xml Debian: http://security.debian.org/pool/updates/main/x/xli/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-332.html Mandrake: http://www.mandrakesecure.net/	XLoadImage Compressed Image Remote Command Execution CAN-2005-0638	High	Gentoo Linux Security Advisory, GLSA 200503-05, March 2, 2005 Fedora Update Notifications, FEDORA-2005-236 & 237, March 18, 2005 Debian Security Advisory, DSA 695-1, March 21, 2005 Turbolinux Security Advisory, TLSA-2005-43, April 19, 2005 RedHat Security Advisory, RHSA-2005:332-10, April 19, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:076, April 21, 2005 **SUSE Security Summary Report,**

	en/ftp.php **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently we are not aware of any exploits for this vulnerability.			**SUSE-SR:2005:012, April 29, 2005**
Nokia Affix Bluetooth Protocol Stack 3.1.1, 3.2	A vulnerability has been reported in the 'affix_sock_register' due to a failure to properly handle user-supplied buffer size parameters, which could let a malicious user obtain elevated privileges. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	Affix Bluetooth Protocol Stack Elevated Privileges CAN-2005-1294	Medium	DMA[2005-0423a] Advisory, April 24, 2005
Novell Evolution 2.0.2, 2.0.3	A remote Denial of Service vulnerability has been reported due to the way messages are processed that contained malformed unicode specifications. Mandrake: http://www.mandrakesecure.net/en/ftp.php **Conectiva:** **ftp://atualizacoes.conectiva.com.br/** Currently we are not aware of any exploits for this vulnerability.	Novell Evolution Remote Denial of Service CAN-2005-0806	Low	Mandrakelinux Security Update Advisory, MDKSA-2005:059, March 17, 2005 **Conectiva Linux Security Announcement, CLA-2005:950, April 27, 2005**
Open WebMail Open WebMail prior to 2.51 20050430	A vulnerability has been reported due to insufficient sanitization of input before using in an 'open()' call, which could let an authenticated remote malicious user execute arbitrary code. Patches available at: http://openwebmail.org/openwebmail/download/cert/patches/SA-05:02/ Currently we are not aware of any exploits for this vulnerability.	Open WebMail Input Validation CAN-2005-1435	High	Security Tracker Alert, 1013859, May 2, 2005
osTicket.com osTicket 1.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported when adding a ticket due to insufficient sanitization of the name and subject fields, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported due to insufficient sanitization of the 'id' and 'cat' parameters before using in a SQL query, which could let a remote malicious user execute arbitrary SQL code; a vulnerability was reported in 'main.php' due to insufficient verification of the 'include_dir' parameter, which could let a local/remote malicious user include arbitrary files; and a vulnerability was reported in 'attachments.php' due to an input validation error when handling the 'file' parameter, which could let a remote malicious user obtain sensitive information. No workaround or patch available at time of publishing. Proofs of Concept exploits have been published.	osTicket Multiple Vulnerabilities CAN-2005-1436 CAN-2005-1437 CAN-2005-1438 CAN-2005-1439	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, : SA15216, May 3, 2005
PHP Group PHP 4.3-4.3.10; Peachtree Linux release 1	A vulnerability has been reported in the 'exif_process_IFD_TAG()' function when processing malformed IFD (Image File Directory) tags, which could let a remote malicious user execute arbitrary code. Upgrades available at: http://ca.php.net/get/php4.3.11.tar.gz/from/a/mirror Ubuntu:	PHP Group Exif Module IFD Tag Integer Overflow CAN-2005-1042	High	Security Focus, 13163, April 14, 2005 Ubuntu Security Notice, USN-112-1, April 14, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005

	http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-405.html** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently, we are not aware of any exploits for this vulnerability.			Fedora Update Notification, FEDORA-2005-315, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 **Turbolinux Security Advisory, TLSA-2005-50, April 28, 2005** **RedHat Security Advisory, RHSA-2005:405-06, April 28, 2005** **SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005**
phpmyAdmin phpMyAdmin 2.6.2	A vulnerability has been reported due to insecure default permissions on the SQL install script, which could let a malicious user obtain unauthorized access. Gentoo: http://security.gentoo.org/glsa/glsa-200504-30.xml There is no exploit code required.	PHPMyAdmin Insecure SQL Install Script CAN-2005-1392	Medium	Gentoo Linux Security Advisory, GLSA 200504-30, April 30, 2005
PostgreSQL PostgreSQL 7.3 through 8.0.2	Two vulnerabilities have been reported: a vulnerability was reported because a remote authenticated malicious user can invoke some client-to-server character set conversion functions and supply specially crafted argument values to potentially execute arbitrary commands; and a remote Denial of Service vulnerability was reported because the 'contrib/tsearch2' module incorrectly declares several functions as returning type 'internal.' Fix available at: http://www.postgresql.org/about/news.315 Currently we are not aware of any exploits for these vulnerabilities.	PostgreSQL Remote Denial of Service & Arbitrary Code Execution CAN-2005-1409 CAN-2005-1410	Low/ High (High if arbitrary code can be executed)	Security Tracker Alert, 1013868, May 3, 2005
Postgrey Postgrey 1.16-1.18, 0.84-9.87	A format string vulnerability has been reported in the 'server.pm' module in the 'log' subroutine, which could let a remote malicious user cause a Denial of Service or execute arbitrary code. Upgrades available at: http://isg.ee.ethz.ch/tools/postgrey/pub/postgrey-1.21.tar.gz **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** Currently, we are not aware of any exploits for this vulnerability.	Postgrey Format String CAN-2005-1127	Low/ High (High if arbitrary code can be executed)	Secunia Advisory, SA14958, April 15, 2005 **SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005**
Red Hat Linux kernel-2.4.20-8.athlon.rpm, 2.4.20-8.i386.rpm, 2.4.20-8.i586.rpm, 2.4.20-8.i686.rpm, kernel-smp-2.4.20-8.athlon.rpm, kernel-smp-2.4.20-8.i586.rpm , kernel-smp-2.4.20-8.i686.rpm ,	A buffer overflow vulnerability exists in the 'ubsec_keysetup()' function in '/drivers/crypto/bcm/pkey.c,' which could let a malicious user cause a Denial of Service or possibly execute arbitrary code. Red Hat: http://rhn.redhat.com/errata/RHSA-2004-549.html	Red Hat BCM5820 Linux Driver Buffer Overflow CAN-2004-0619	High/Low (High if arbitrary code can be executed; and Low if a DoS)	Security Tracker Alert, 1010575, June 24, 2004 Red Hat Advisory: RHSA-2004:549-10, December 2, 2004 **RedHat Security Advisory, RHSA-2005:283-15, April 28, 2005**

kernel-source-2.4.20-8.i386.rpm, Linux 8.0, i686, i386	**RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-283.html** Currently we are not aware of any exploits for this vulnerability.			
RedHat Enterprise Linux WS 3, ES 3, AS 3	A vulnerability has been reported in the Native POSIX Threading Library (NPTL) due to a design error, which could let a malicious user cause a Denial of Service or obtain sensitive information. RedHat: http://rhn.redhat.com/errata/RHSA-2005-293.html Currently we are not aware of any exploits for this vulnerability.	RedHat Enterprise Linux Native POSIX Threading Library CAN-2005-0403	Low/ Medium (Medium if sensitive information can be obtained)	RedHat Security Advisory, RHSA-2005:293-16, April 22, 2005
Rob Flynn Gaim 1.0-1.0.2, 1.1.1, 1.1.2	Multiple remote Denial of Service vulnerabilities have been reported when a remote malicious ICQ or AIM user submits certain malformed SNAC packets; and a vulnerability exists when parsing malformed HTML data. Upgrades available at: http://gaim.sourceforge.net/downloads.php Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/g/gaim/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-03.xml Mandrake: Http://www.mandrakesecure.net/en/advisories/ RedHat: http://rhn.redhat.com/errata/RHSA-2005-215.html Conectiva: ftp://atualizacoes.conectiva.com.br/ Peachtree: http://peachtree.burdell.org/updates/ **Debian:** **http://security.debian.org/pool/updates/main/g/gaim/** There is no exploit code required.	Gaim Multiple Remote Denials of Service CAN-2005-0472 CAN-2005-0473	Low	Gaim Advisory, February 17, 2005 Fedora Update Notifications, FEDORA-2005-159 & 160, February 21, 2005 US-CERT VU#839280 US-CERT VU#523888 Ubuntu Security Notice, USN-85-1 February 25, 2005 Gentoo Linux Security Advisory, GLSA 200503-03, March 1, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:049, March 4, 2005 RedHat Security Advisory, RHSA-2005:215-11, March 10, 2005 Conectiva Linux Security Announcement, CLA-2005:933, March 14, 2005 Peachtree Linux Security Notice, PLSN-0002, April 21, 2005 **Debian Security Advisory, DSA 716-1, April 27, 2005**
Robert Styma Consulting Ce/Ceterm (ARPUS/Ce) 2.x	Several vulnerabilities have been reported: a buffer overflow vulnerability was reported when a specially crafted 'XAPPLRESLANGPATH' or 'XAPPLRESDIR' environment variable is submitted, which could let malicious user execute arbitrary code; and a race condition vulnerability was reported due to the insecure creation of the 'ce_edit_log' temporary file, which could let a malicious user overwrite arbitrary files. No workaround or patch available at time of publishing. Exploit scripts have been published.	Robert Styma Consulting ARPUS/Ce Buffer Overflow & Race Condition CAN-2005-1395 CAN-2005-1396	High	Security Tracker Alert, 1013855, May 2, 2005
Rootkit.nl Rootkit Hunter 1.2-1.2.3	Several vulnerabilities have been reported because temporary files are insecurely opened or created due to a design error, which could let a malicious user corrupt arbitrary files with elevated privileges. Gentoo: http://security.gentoo.org/glsa/glsa-200504-25.xml There is no exploit code required.	Rootkit Hunter Insecure Temporary File Creation CAN-2005-1270	Medium	Secunia Advisory, SA15127, April 27, 2005 Gentoo Linux Security Advisory GLSA 200504-25, April 26, 2005

Survivor Survivor 0.9.5 a	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code. Upgrade available at: http://www.columbia.edu/acis/dev/projects/survivor/dl/survivor-0.9.6.tar.gz There is no exploit code required.	Survivor Cross-Site Scripting CAN-2005-1388	High	Security Focus, 13415, April 28, 2005
Vladislav Bogdanov SNMP Proxy Daemon 0.4-0.4.5	A format string vulnerability has been reported in SNMPPD due to insufficient sanitization of user-supplied input before using in a formatted printing function, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. **An exploit script has been published.**	SNMPPD SNMP Proxy Daemon Remote Format String CAN-2005-1246	High	INetCop Security Advisory #2005-0x82-027, April 24, 2005 **Security Focus, 13348, April 29,2005**

[back to top]

Multiple Operating Systems - Windows / UNIX / Linux / Other

Vendor & Software Name	Vulnerability - Impact Patches - Workarounds Attacks Scripts	Common Name / CVE Reference	Risk	Source
BakBone NetVault 7.1	A vulnerability has been reported because 'vstatsmngr.exe' can be manipulated to obtain elevated privileges. No workaround or patch available at time of publishing. An exploit script has been published.	BakBone NetVault 'NVStatsMngr.EXE' Elevated Privileges CAN-2005-1372	Medium	Security Focus, 13408, April 27, 2005
BEA Systems, Inc, WebLogic Express 8.x, WebLogic Server 8.x	A Cross-Site Scripting vulnerability has been reported in the 'JndiFramesetAction' function due to insufficient validation of the 'server' parameter, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; hover, a Proof of Concept exploit has been published.	BEA WebLogic Server & WebLogic Express Cross-Site Scripting CAN-2005-1380	High	Security Tracker Alert, 1013817, April 26, 2005
Claroline Claroline 1.5.3, 1.6 rc1, 1.6 beta	Multiple input validation vulnerabilities have been reported: Cross-Site Scripting vulnerabilities were reported in the '/exercise_result.php,' 'exercice_submit.php,' 'myagenda.php,' 'agenda.php,' 'user_access_details.php,' 'toolaccess_details.php,' 'learningPathList.php,' 'learningPathAdmin.php,' 'learningPath.php,' and 'userLog.php' pages due to insufficient input validation, which could let a remote malicious user execute arbitrary HTML and script code; SQL injection vulnerabilities were reported in 'learningPath.php (3),' 'exercises_details.php,' 'learningPathAdmin.php,' 'learnPath_details.php,' 'userInfo.php (2),' 'modules_pool.php,' and 'module.php' due to insufficient input validation, which could let a remote malicious user execute arbitrary SQL code; multiple Directory Traversal vulnerabilities were reported in 'claroline/document/document.php' and 'claroline/learnPath/insertMyDoc.php' due to insufficient input validation, which could let remote malicious project administrators (teachers) upload files in arbitrary folders or copy/move/delete (then view) files of arbitrary folders; and remote file inclusion vulnerabilities were reported due to insufficient verification, which could let a remote malicious user include arbitrary files from external and local resources. Upgrades available at: http://www.claroline.net/dlarea/ There is no exploit code required; however, Proofs of Concept exploits have been published.	Claroline Multiple Vulnerabilities CAN-2005-1374 CAN-2005-1375 CAN-2005-1376 CAN-2005-1377	Medium/ High (High if arbitrary code can be executed)	Zone-H Research Center Security Advisory, 200501, April 27, 2005
codetosell.com ViArt Shop Enterprise 2.x	Multiple vulnerabilities have been reported: a Cross-Site Scripting vulnerability was reported in the 'basket.php,' 'forum.php,' 'page.php,' 'reviews.php,' 'products.php,' and 'news_view.php' scripts due to insufficient validation of user-supplied input, which could let a remote malicious user execute arbitrary HTML and script code; and a Cross-SIte Scripting vulnerability was reported in the 'forum_new_thread.php' script due to insufficient sanitization of input passed to the nickname, email, topic and message fields and the nickname and message fields in 'forum_threads.php,' which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concepts have been published.	ViArt Shop Enterprise Cross-Site Scripting CAN-2005-1440	High	Secunia Advisory, SA15181, May 2, 2005

dream4 Koobi CMS 4.2.3	An SQL injection vulnerability was reported in the 'index.php' due to insufficient sanitization of the 'p' and 'q' parameters, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concept exploits have been published.	Dream4 Koobi CMS Index.PHP P Parameter SQL Injection CAN-2005-1373	High	Bugtraq, 397057, April 27, 2005
Ethereal Group Ethereal 0.9-0.9.16, 0.10-0.10.9	Multiple vulnerabilities have been reported: a buffer overflow vulnerability has been reported in the Etheric dissector, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; a remote Denial of Service vulnerability has been reported in the GPRS-LLC dissector if the 'ignore cipher bit' option is enabled; a buffer overflow vulnerability has been reported in the 3GPP2 A11 dissector, which could let a remote malicious user cause a Denial of Service or execute arbitrary code; and remote Denial of Service vulnerabilities have been reported in the JXTA and sFLow dissectors. Upgrades available at: http://www.ethereal.com/download.html Gentoo: http://security.gentoo.org/glsa/glsa-200503-16.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Mandrake: http://www.mandrakesecure.net/en/ftp.php RedHat: http://rhn.redhat.com/errata/RHSA-2005-306.html ALT Linux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Conectiva: ftp://atualizacoes.conectiva.com.br/ **Debian: http://security.debian.org/pool/updates/main/e/ethereal/** A Denial of Service Proof of Concept exploit script has been published.	Ethereal Etheric/ GPRS-LLC/IAPP/ JXTA/s Flow Dissector Vulnerabilities CAN-2005-0704 CAN-2005-0705 CAN-2005-0739 CAN-2005-0765 CAN-2005-0766	Low/ HIgh (High if arbitrary code can be executed)	Ethereal Advisory, enpa-sa-00018, March 12, 2005 Gentoo Linux Security Advisory, GLSA 200503-16, March 12, 2005 Fedora Update Notifications, FEDORA-2005-212 & 213, March 16, 2005 Mandrakelinux Security Update Advisory, MDKSA-2005:053, March 16, 2005 RedHat Security Advisory, RHSA-2005:306-10, March 18, 2005 Conectiva Security Linux Announcement, CLA-2005:942, March 28, 2005 ALTLinux Security Advisory, March 29, 2005 **Debian Security Advisory, DSA 718-1, April 28, 2005**
GrayCMS GrayCMS 1.1	A vulnerability has been reported in 'error.php' due to insufficient sanitization of user-supplied input, which could let a remote malicious user execute arbitrary code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	GrayCMS Error.PHP Remote Code Execution CAN-2005-1360	High	Secunia Advisory, SA15133, April 27, 2005
Hewlett Packard Company Radia Management Portal 1.0, 2.0	A vulnerability has been reported in the Radia Management Agent due to an unspecified flaw, which could let a remote malicious user cause a Denial of Service or execute arbitrary code with SYSTEM privileges on a Windows platform and elevated privileges on UNIX-based platforms. Updates available at: http://support.openview.hp.com Currently we are not aware of any exploits for this vulnerability.	HP OpenView Radia Management Portal Remote Command Execution CAN-2005-1370	Low/ High (High if arbitrary code can be executed)	HP Security Bulletin, HPSBMA01138, April 28, 2005
Horde Project Horde Kronolith Module	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/kronolith/download/ **Gentoo: http://security.gentoo.org/glsa/glsa-200505-01.xml** There is no exploit code required.	Horde Kronolith Module Parent Frame Page Title Cross-Site Scripting CAN-2005-1314	High	Secunia Advisory, SA15080, April 25, 2005 **Gentoo Linux Security Advisory, GLSA 200505-01, May 2, 2005**

Horde Project Horde Passwd Module 2.x	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/passwd/download/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-01.xml** There is no exploit code required.	Horde Passwd Module Parent Frame Page Title Cross-Site Scripting CAN-2005-1313	High	Secunia Advisory, SA15075, April 25, 2005 **Gentoo Linux Security Advisory, GLSA 200505-01, May 2, 2005**
Horde Project HordeTurba Module 1.x	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/turba/download/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-01.xml** There is no exploit code required.	Horde Turba Module Parent Frame Page Title Cross-Site Scripting CAN-2005-1315	High	Secunia Advisory, SA15074, April 25, 2005 **Gentoo Linux Security Advisory, GLSA 200505-01, May 2, 2005**
Horde Project Horde Accounts Module 2.1, 2.1.1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/accounts/download/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-01.xml** There is no exploit code required.	Horde Accounts Module Parent Frame Page Title Cross-Site Scripting CAN-2005-1316	High	Secunia Advisory, SA15081, April 25, 2005 **Gentoo Linux Security Advisory, GLSA 200505-01, May 2, 2005**
Horde Project Horde Chora 1.1-1.2.2	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/chora/download/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-01.xml** There is no exploit code required.	Horde Chora Parent Frame Page Title Cross-Site Scripting CAN-2005-1317	High	Secunia Advisory, SA15083, April 25, 2005 **Gentoo Linux Security Advisory, GLSA 200505-01, May 2, 2005**
Horde Project Horde Forwards Module 2.1-2.2.1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/forwards/download/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-01.xml** There is no exploit code required.	Horde Forwards Module Parent Frame Page Title Cross-Site Scripting CAN-2005-1318	High	Secunia Advisory, SA15082, April 25, 2005 **Gentoo Linux Security Advisory, GLSA 200505-01, May 2, 2005**
Horde Project Horde IMP Webmail Client 3.x	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: ftp://ftp.horde.org/pub/imp/imp-3.2.8.tar.gz **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-01.xml** There is no exploit code required.	Horde IMP Webmail Client Parent Frame Page Title Cross-Site Scripting CAN-2005-1319	High	Secunia Advisory, SA15080, April 25, 2005 **Gentoo Linux Security Advisory, GLSA 200505-01, May 2, 2005**

Horde Project Horde Mnemo 1.1-1.1.3	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/mnemo/download/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-01.xml** There is no exploit code required.	Horde Mnemo Parent Frame Page Title Cross-Site Scripting CAN-2005-1320	High	Secunia Advisory, SA15078, April 25, 2005 **Gentoo Linux Security Advisory, GLSA 200505-01, May 2, 2005**
Horde Project Horde Vacation 2.0-2.2.1	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/vacation/download/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-01.xml** There is no exploit code required.	Horde Vacation Parent Frame Page Title Cross-Site Scripting CAN-2005-1321	High	Secunia Advisory, SA15073, April 25, 2005 **Gentoo Linux Security Advisory, GLSA 200505-01, May 2, 2005**
Horde Project HordeNag 1.1-1.1.2	A Cross-Site Scripting vulnerability has been reported due to insufficient sanitization of input passed to a parent's frame page title, which could let a remote malicious user execute arbitrary HTML and script code. Upgrades available at: http://www.horde.org/nag/download/ **Gentoo:** **http://security.gentoo.org/glsa/glsa-200505-01.xml** There is no exploit code required.	Horde Nag Parent Frame Page Title Cross-Site Scripting CAN-2005-1322	High	Secunia Advisory, SA15079, April 25, 2005 **Gentoo Linux Security Advisory, GLSA 200505-01, May 2, 2005**
IBM Lotus Domino 6.0.x, 6.5.x; prior to 6.0.5, prior to 6.5.4	An input validation vulnerability has been reported in the '@SetHTTPHeader' function when invoked by specially crafted code, which could let a malicious user conduct HTTP response splitting attacks. Update information available at: http://www-1.ibm.com/support/docview.wss?rs=463&uid=swg21202437 Currently we are not aware of any exploits for this vulnerability.	Lotus Domino '@SetHTTPHeader' Function HTTP Response Splitting CAN-2005-1405	Medium	Security Tracker Alert, 1013839, April 29, 2005
IBM Lotus Domino 6.0.x, 6.5.x; prior to 6.0.5, prior to 6.5.4	A format string vulnerability has been reported when processing the Notes protocol (NRPC), which could let a remote malicious user cause a Denial of Service. Update information available at: http://www-1.ibm.com/support/docview.wss?rs=463&uid=swg21202525 Currently we are not aware of any exploits for this vulnerability	Lotus Domino NRPC Protocol Format String CAN-2005-1441	Low	Security Tracker Alert, 1013842, April 29, 2005
IBM Lotus Notes 6.0.x, 6.5.x; prior to 6.0.5, prior to 6.5.4	A Denial of Service vulnerability has been reported because a malicious user can modify the 'NOTES.INI' file. Update information available at: http://www-1.ibm.com/support/docview.wss?rs=463&uid=swg21202526 Currently we are not aware of any exploits for this vulnerability.	IBM Lotus Notes 'notes.ini' File Denial of Service CAN-2005-1442	Low	Security Tracker Alert, 1013841, April 29, 2005
Invision Power Services Invision Power Board 2.0.3, 2.1 Alpha 2	A Cross-Site Scripting vulnerability has been reported due to insufficient validation of user-supplied input in certain URL parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing.	Invision Power Board Remote Cross-Site Scripting CAN-2005-1443	High	Security Tracker Alert, 1013863, May 2, 2005

	A Proof of Concept exploit has been published.			
Just William's Amazon Webstore 04050100	Cross-Site Scripting vulnerabilities have been reported in the 'index.php' and 'closeup.php' scripts due to insufficient validation of the 'CurrentIsExpanded,' 'image,' "searchFor,' and 'currentNumber' parameters, which could let a remote malicious user execute arbitrary HTML and script code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	JustWilliam's Amazon Webstore Cross-Site Scripting CAN-2005-1403	High	Security Tracker Alert, 1013836, April 29, 2005
Morgan Harvey SitePanel 2.x	Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient sanitization of unspecified input, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability as reported in '5.php' due to insufficient verification of the 'id' parameter, which could let a remote malicious user delete arbitrary files; a vulnerability was reported in 'index.php' due to insufficient verification of the 'lang' parameter, which could let a remote malicious user include arbitrary files; an input validation vulnerability was reported when handling attachments in trouble tickets, which could let a remote malicious user upload arbitrary files; and a vulnerability was reported in 'main.php' due to insufficient verification of the 'p' parameter, which could let a remote malicious user include arbitrary files. Update available at: http://www.sitepanel2.com/ Proofs of Concept exploits have been published.	SitePanel Multiple Vulnerabilities CAN-2005-1444 CAN-2005-1445 CAN-2005-1446 CAN-2005-1447	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA15213, May 3, 2005
Mozilla.org Firefox 1.x, 0.x, Mozilla 1.7.x, 1.6, 1.5, 1.4, 1.3, 1.2, 1.1, 1.0, 0.x	A vulnerability exists because a website can inject content into another site's window if the target name of the window is known, which could let a remote malicious user spoof the content of websites Gentoo: http://security.gentoo.org/glsa/glsa-200503-10.xml Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123 **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-384.html** A Proof of Concept exploit has been published. Vulnerability has appeared in the press and other public media.	Mozilla Browser and Mozilla Firefox Remote Window Hijacking CAN-2004-1156	Medium	Secunia SA13129, December 8, 2004 Gentoo Linux Security Advisory GLSA 200503-10, March 4, 2005 Fedora Update Notifications, FEDORA-2005-248 & 249, 2005-03-23 Fedora Update Notifications, FEDORA-2005-251 & 253, March 25, 2005 Gentoo Linux Security Advisory, GLSA 200503-30, March 25, 2005 Slackware Security Advisory, March 28, 2005 **RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005**
Mozilla.org Mozilla Browser 1.0-1.0.2, 1.1-1.7.6, Firefox 0.8-0.10.1, 1.0.1, 1.0.2	Multiple vulnerabilities have been reported: a vulnerability was reported in the 'EMBED' tag for non-installed plugins when processing the 'PLUGINSPAGE' attribute due to an input validation error, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because blocked popups that are opened through the GUI incorrectly run with 'chrome' privileges, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the global scope of a window or tab are not cleaned properly before navigating to a new web site, which could let a remote malicious user execute arbitrary code; a vulnerability was reported because the URL of a 'favicons' icon for a web site isn't verified before changed via JavaScript, which could let a remote malicious user execute arbitrary code with elevated privileges; a vulnerability was reported because the search plugin action URL is not properly verified before used to perform a search, which could let a remote malicious user execute arbitrary code; a vulnerability was reported due to the way links are opened in a sidebar when using the '_search' target, which could let a remote malicious user execute arbitrary code; several input validation vulnerabilities were reported when handling invalid type parameters passed to 'InstallTrigger' and 'XPInstall' related objects, which could let a remote malicious user execute arbitrary code; and vulnerabilities were reported due to insufficient validation of DOM nodes in certain privileged UI code, which could let	Mozilla Suite / Firefox Multiple Vulnerabilities CAN-2005-0752 CAN-2005-1153 CAN-2005-1154 CAN-2005-1155 CAN-2005-1156 CAN-2005-1157 CAN-2005-1158 CAN-2005-1159 CAN-2005-1160	High	Mozilla Foundation Security Advisories, 2005-35 - 2005-41, April 16, 2005 Gentoo Linux Security Advisory, GLSA 200504-18, April 19, 2005 US-CERT VU#973309 RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005-386., April 21 & 26, 2005 Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005

	a remote malicious user execute arbitrary code. Upgrades available at: http://www.mozilla.org/products/firefox/ http://www.mozilla.org/products/mozilla1.x/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-18.xml RedHat: http://rhn.redhat.com/errata/RHSA-2005-383.html http://rhn.redhat.com/errata/RHSA-2005-386.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-384.html** There is no exploit code required.			US-CERT VU#519317 **SUSE Security Announcement, SUSE-SA:2005:028, April 27, 2005** **RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005**
Mozilla.org Mozilla Suite prior to 1.7.6, Firefox prior to 1.0.2	A vulnerability has been reported when processing drag and drop operations due to insecure XUL script loading, which could let a remote malicious user execute arbitrary code. Mozilla Browser: http://www.mozilla.org/products/mozilla1.x/ Firefox: http://www.mozilla.org/products/firefox/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml http://security.gentoo.org/glsa/glsa-200503-31.xml Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123 **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-384.html** A Proof of Concept exploit has been published.	Mozilla Suite/ Firefox Drag and Drop Arbitrary Code Execution CAN-2005-0401	High	Mozilla Foundation Security Advisory 2005-32, March 23, 2005 **RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005**

Mozilla Mozilla 0.x, 1.0, 1.1, 1.2, 1.3, 1.4, 1.5, 1.6, 1.7.x Mozilla Firefox 0.x Mozilla Thunderbird 0.x	Multiple vulnerabilities exist in Firefox, Mozilla and Thunderbird that can permit users to bypass certain security restrictions, conduct spoofing and script insertion attacks and disclose sensitive and system information. Mozilla: Update to version 1.7.5: http://www.mozilla.org/products/mozilla1.x/ Firefox: Update to version 1.0: http://www.mozilla.org/products/firefox/ Thunderbird: Update to version 1.0: http://www.mozilla.org/products/thunderbird/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ Slackware: http://slackware.com/security/viewer.php?l=slackware-security&y=2005&m=slackware-security.000123 **RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html** Currently we are not aware of any exploits for these vulnerabilities.	Mozilla Firefox, Mozilla, and Thunderbird Multiple Vulnerabilities CAN-2005-0141 CAN-2005-0143 CAN-2005-0144 CAN-2005-0145 CAN-2005-0146 CAN-2005-0147 CAN-2005-0148 CAN-2005-0149 CAN-2005-0150	Medium/ High (High if arbitrary code can be executed)	Mozilla Foundation Security Advisory 2005-01, 03, 04, 07, 08, 09, 10, 11, 12 Fedora Update Notification, FEDORA-2005-248, 249, 251, 253, March 23 & 25, 2005 Slackware Security Advisory, SSA:2005-085-01, March 27, 2005 **RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005**
Mozilla Mozilla Firefox 1.0 and 1.0.1	A vulnerability exists that could let remote malicious users conduct Cross-Site Scripting attacks. This is due to missing URI handler validation when dragging an image with a "javascript:" URL to the address bar. Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml **RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html** A Proof of Concept exploit has been published.	Mozilla Firefox Image Javascript URI Dragging Cross-Site Scripting Vulnerability CAN-2005-0591	High	Secunia SA14406, March 1, 2005 Gentoo Linux Security Advisory, GLSA 200503-30, March 25, 2005 **RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005**
Multiple Vendors Mozilla Firefox 1.0; Gentoo Linux; Thunderbird 0.6, 0.7-0.7.3, 0.8, 0.9, 1.0, 1.0.1; Netscape Netscape 7.2	There are multiple vulnerabilities in Mozilla Firefox. A remote user may be able to cause a target user to execute arbitrary operating system commands in certain situations or access access content from other windows, including the 'about:config' settings. This is due to a hybrid image vulnerability that allows batch statements to be dragged to the desktop and because tabbed javascript vulnerabilities let remote users access other windows. A fix is available via the CVS repository Fedora: ftp://aix.software.ibm.com/aix/efixes/security/perl58x.tar.Z Red Hat: http://rhn.redhat.com/errata/RHSA-2005-176.html Gentoo: http://www.gentoo.org/security/en/glsa/glsa-200503-10.xml Thunderbird: http://download.mozilla.org/?product=thunderbird-1.0.2&os=win<=en-US Gentoo: http://security.gentoo.org/glsa/glsa-200503-30.xml **RedHat: http://rhn.redhat.com/errata/RHSA-2005-384.html** A Proof of Concept exploit has been published.	Mozilla Firefox Multiple Vulnerabilities CAN-2005-0230 CAN-2005-0231 CAN-2005-0232	High	Security Tracker Alert ID: 1013108, February 8, 2005 Fedora Update Notification, FEDORA-2005-182, February 26, 2005 Red Hat RHSA-2005:176-11, March 1, 2005 Gentoo, GLSA 200503-10, March 4, 2005 Security Focus, 12468, March 22, 2005 Gentoo Linux Security Advisory, GLSA 200503-30, March 25, 2005 **RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005**
Multiple Vendors Mozilla.org Mozilla Browser 1.7.6, Firefox 1.0.1, 1.0.2;	A vulnerability has been reported in the javascript implementation due to improper parsing of lamba list regular expressions, which could a remote malicious user obtain sensitive information.	Mozilla Suite/Firefox JavaScript Lambda Information	Medium	Security Tracker Alert, 1013635, April 4, 2005 Security Focus, 12988,

K-Meleon K-Meleon 0.9; Netscape 7.2; K-Meleon 0.9	The vendor has issued a fix, available via CVS. RedHat: http://rhn.redhat.com/errata/RHSA-2005-383.html http://rhn.redhat.com/errata/RHSA-2005-386.html Slackware: http://www.mozilla.org/projects/security/known-vulnerabilities.html TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/ **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **RedHat:** **http://rhn.redhat.com/errata/RHSA-2005-384.html** There is no exploit code required; however, a Proof of Concept exploit has been published.	Disclosure CAN-2005-0989		April 16, 2005 RedHat Security Advisories, RHSA-2005:383-07 & RHSA-2005:386-08, April 21 & 26, 2005 Turbolinux Security Advisory, TLSA-2005-49, April 21, 2005 Slackware Security Advisory, SSA:2005-111-04, April 22, 2005 **SUSE Security Announcement, SUSE-SA:2005:028, April 27, 2005** **RedHat Security Advisory, RHSA-2005:384-11, April 28, 2005**
Multiple Vendors ALT Linux Compact 2.3, Junior 2.3; Apple Mac OS X 10.0-10.0.4, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8, Mac OS X Server 10.0, 10.1-10.1.5, 10.2-10.2.8, 10.3-10.3.8; MIT Kerberos 5 1.0, 5 1.0.6, 5 1.0.8, 51.1-5 1.4; Netkit Linux Netkit 0.9-0.12, 0.14-0.17, 0.17.17; Openwall GNU/*/Linux (Owl)-current, 1.0, 1.1; FreeBSD 4.10-PRERELEASE, 2.0, 4.0 .x, -RELENG, alpha, 4.0, 4.1, 4.1.1 -STABLE, -RELEASE, 4.1.1, 4.2, -STABLEpre122300, -STABLEpre050201, 4.2 -STABLE, -RELEASE, 4.2, 4.3 -STABLE, -RELENG, 4.3 -RELEASE-p38, 4.3 -RELEASE, 4.3, 4.4 -STABLE, -RELENG, -RELEASE-p42, 4.4, 4.5 -STABLEpre2002-03-07, 4.5 -STABLE, -RELENG, 4.5 -RELEASE-p32, 4.5 -RELEASE, 4.5, 4.6 -STABLE, -RELENG, 4.6 -RELEASE-p20, 4.6 -RELEASE, 4.6, 4.6.2, 4.7 -STABLE, 4.7 -RELENG, 4.7 -RELEASE-p17, 4.7 -RELEASE, 4.7, 4.8 -RELENG, 4.8 -RELEASE-p7, 4.8 -PRERELEASE, 4.8, 4.9 -RELENG, 4.9 -PRERELEASE, 4.9, 4.10 -RELENG, 4.10 -RELEASE, 4.10, 4.11 -STABLE, 5.0 -RELENG, 5.0, 5.1 -RELENG, 5.1 -RELEASE-p5, 5.1 -RELEASE, 5.1, 5.2 -RELENG, 5.2 -RELEASE, 5.2, 5.2.1 -RELEASE, 5.3 -STABLE, 5.3 -RELEASE, 5.3, 5.4 -PRERELEASE; SuSE Linux 7.0, sparc, ppc, i386, alpha, 7.1, x86, sparc, ppc, alpha, 7.2, i386	Two buffer overflow vulnerabilities have been reported in Telnet: a buffer overflow vulnerability has been reported in the 'slc_add_reply()' function when a large number of specially crafted LINEMODE Set Local Character (SLC) commands is submitted, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported in the 'env_opt_add()' function, which could let a remote malicious user execute arbitrary code. ALTLinux: http://lists.altlinux.ru/pipermail/security-announce/2005-March/000287.html Apple: http://wsidecar.apple.com/cgi-bin/nph-reg3rdpty1.pl/product=05529&platform=osx&method=sa/SecUpd2005-003Pan.dmg Debian: http://security.debian.org/pool/updates/main/n/netkit-telnet/ Fedora: http://download.fedora.redhat.com/pub/fedora/linux/core/updates/ FreeBSD: ftp://ftp.FreeBSD.org/pub/FreeBSD/CERT/patches/SA-05:01/ MIT Kerberos: http://web.mit.edu/kerberos/advisories/2005-001-patch_1.4.txt Netkit: ftp://ftp.uk.linux.org/pub/linux/Networking/netkit/ Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml RedHat: http://rhn.redhat.com/errata/RHSA-2005-327.html Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57755-1 SUSE: ftp://ftp.SUSE.com/pub/SUSE Ubuntu: http://security.ubuntu.com/ubuntu/	Telnet Client 'slc_add_reply()' & 'env_opt_add()' Buffer Overflows CAN-2005-0468 CAN-2005-0469	High	iDEFENSE Security Advisory, March 28, 2005 US-CERT VU#291924 Mandrakelinux Security Update Advisory, MDKSA-2005:061, March 30, 2005 Gentoo Linux Security Advisories, GLSA 200503-36 & GLSA 200504-01, March 31 & April 1, 2005 Debian Security Advisory, DSA 703-1, April 1, 2005 US-CERT VU#341908 Gentoo Linux Security Advisory, GLSA 200504-04, April 6, 2005 SGI Security Advisory, 20050401-01-U, April 6, 2005 Sun(sm) Alert Notification, 57761, April 7, 2005 SCO Security Advisory, SCOSA-2005.21, April 8, 2005 **Avaya Security Advisory, ASA-2005-088, April 27, 2005** **Gentoo Linux Security Advisory, GLSA 200504-28, April 28, 2005** **Turbolinux Security Advisory, TLSA-2005-52, April 28, 2005** **Sun(sm) Alert Notification, 57761, April 29, 2005**

	pool/main/n/netkit-telnet/ OpenBSD: http://www.openbsd.org/errata.html#telnet Mandrake: http://www.mandrakesecure.net/en/ftp.php Gentoo: http://security.gentoo.org/glsa/glsa-200503-36.xml http://security.gentoo.org/glsa/glsa-200504-01.xml Debian: http://security.debian.org/pool/updates/main/k/krb5/ Gentoo: http://security.gentoo.org/glsa/glsa-200504-04.xml SGI: ftp://oss.sgi.com/projects/sgi_propack/download/3/updates/ SCO: ftp://ftp.sco.com/pub/updates/UnixWare/SCOSA-2005.21 Sun: http://sunsolve.sun.com/search/document.do?assetkey=1-26-57761-1 Openwall: http://www.openwall.com/Owl/CHANGES-current.shtml **Avaya:** **http://support.avaya.com/elmodocs2/security/ASA-2005-088_RHSA-2005-330.pdf** **Gentoo:** **http://security.gentoo.org/glsa/glsa-200504-28.xml** **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-57761-1** **OpenWall:** **http://www.openwall.com/Owl/CHANGES-current.shtml** Currently we are not aware of any exploits for these vulnerabilities.			
Multiple Vendors MPlayer 1.0pre6 & prior; Xine 0.9.9-1.0; Peachtree Linux release 1	Several vulnerabilities have been reported: a buffer overflow vulnerability has been reported due to a boundary error when processing lines from RealMedia RTSP streams, which could let a remote malicious user execute arbitrary code; and a buffer overflow vulnerability has been reported due to a boundary error when processing stream IDs from Microsoft Media Services MMST streams, which could let a remote malicious user execute arbitrary code. Patches available at: http://www.mplayerhq.hu/MPlayer/patches/rtsp_fix_20050415.diff Gentoo: http://security.gentoo.org/glsa/glsa-200504-19.xml Patches available at: http://cvs.sourceforge.net/viewcvs.py/xine/xinelib/src/input/ **Gentoo:**	MPlayer RTSP & MMST Streams Buffer Overflow CAN-2005-1195	High	Security Tracker Alert,1013771, April 20, 2005 Gentoo Linux Security Advisory, GLSA 200504-19, April 20, 200 Peachtree Linux Security Notice, PLSN-0003, April 21, 2005 Xine Security Announcement, XSA-2004-8, April 21, 2005 **Gentoo Linux Security Advisory, GLSA 200504-27, April 26,**

	http://security.gentoo.org/glsa/glsa-200504-27.xml **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** **Slackware:** **ftp://ftp.slackware.com/pub/slackware/** Currently we are not aware of any exploits for these vulnerabilities.			**2005** **SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005** **Slackware Security Advisory, SSA:2005-121-02, May 3, 2005**
Multiple Vendors See US-CERT VU#222750 for complete list	Multiple vendor implementations of TCP/IP Internet Control Message Protocol (ICMP) do not adequately validate ICMP error messages, which could let a remote malicious user cause a Denial of Service. Cisco: http://www.cisco.com/warp/public/707/cisco-sa-20050412-icmp.shtml IBM: ftp://aix.software.ibm.com/aix/efixes/security/icmp_efix.tar.Z RedHat: http://rhn.redhat.com/errata/ **Sun:** **http://sunsolve.sun.com/search/document.do?assetkey=1-26-57746-1** Currently we are not aware of any exploits for these vulnerabilities.	Multiple Vendor TCP/IP Implementation ICMP Remote Denial of Service CAN-2004-1060 CAN-2004-0790 CAN-2004-0791	Low	**US-CERT VU#222750** **Sun(sm) Alert Notification, 57746, April 29, 2005** **US-CERT VU#415294**
Multiple Vendors Squid Web Proxy Cache 2.3, STABLE2, STABLE4-STABLE7, 2.5, STABLE1, STABLE3-STABLE9	A remote Denial of Service vulnerability has been reported when a malicious user prematurely aborts a connection during a PUT or POST request. Patches available at: http://www1.uk.squid-cache.org/Versions/v2/2.5/bugs/squid-2.5.STABLE7-post.patch Conectiva: ftp://atualizacoes.conectiva.com.br/ Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/s/squid/ **TurboLinux:** **ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** **Mandrake:** **http://www.mandrakesecure.net/en/ftp.php** **SUSE:** **ftp://ftp.SUSE.com/pub/SUSE** There is no exploit code required.	Squid Proxy Aborted Connection Remote Denial of Service CAN-2005-0718	Low	Security Focus, 13166, April 14, 2005 **Turbolinux Security Advisory, TLSA-2005-53, April 28, 2005** **Mandriva Linux Security Update Advisory, MDKSA-2005:078, April 29, 2005** **SUSE Security Summary Report, SUSE-SR:2005:012, April 29, 2005**
MyPHP Forum MyPHP Forum 1.0	A vulnerability has been reported in 'post.php' and 'privmsg.php' because the username can be spoofed by modifying the 'nbuser' and 'sender' parameter, which could let a remote malicious user conduct spoofing attacks. No workaround or patch available at time of publishing. There is no exploit code required.	MyPHP Forum Sender Spoofing CAN-2005-1404	Medium	Secunia Advisory, SA15166, April 28, 2005
Oracle Corporation Oracle Application Server 10g, Oracle9i Application Server, Oracle9iAS Web Cache	Several vulnerabilities have been reported: a vulnerability was reported in 'webcacheadmin' on port 4000 due to insufficient sanitization of the 'cache_dump_file' and 'PartialPageErrorPage' parameters, which could let a remote malicious user execute arbitrary HTML and script code; a vulnerability was reported in the 'cache_dump_file' parameter, which could let a remote malicious user corrupt arbitrary files; and a vulnerability was reported because restricted URLs on port 7779 can be accessed via the Web Cache on port 7778. The vendor has reportedly fixed the vulnerabilities silently. Ensure that the latest patches have been installed. Proofs of Concept exploits have been published.	Oracle Web Cache / Application Server Vulnerabilities CAN-2005-1381 CAN-2005-1382 CAN-2005-1383	Medium	Red-Database-Security GmbH Research Advisories, April 28, 2005

OXPUS.de Notes mod	An SQL injection vulnerability has been reported in the 'posting_notes.php' module due to insufficient validation of the 'post_id' parameter, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, a Proof of Concept exploit has been published.	phpBB Notes Mod 'posting_notes.php' Input Validation CAN-2005-1378	High	GulfTech Security Research Team Advisory, April 28, 2005
PHP Group PHP 4.0-4.0.7, 4.0.7 RC1-RC3, 4.1 .0-4.1.2, 4.2 .0-4.2.3, 4.3-4.3.8, 5.0 candidate 1-3, 5.0 .0-5.0.2	A vulnerability exists in the 'open_basedir' directory setting due to a failure of the cURL module to properly enforce restrictions, which could let a malicious user obtain sensitive information. Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ FedoraLegacy: http://download.fedoralegacy.org/redhat/ **RedHat: http://rhn.redhat.com/errata/RHSA-2005-405.html** There is no exploit code required; however, a Proof of Concept exploit has been published.	PHP cURL Open_Basedir Restriction Bypass CAN-2004-1392	Medium	Security Tracker Alert ID, 1011984, October 28, 2004 Ubuntu Security Notice, USN-66-1, January 20, 2005 Ubuntu Security Notice, USN-66-2, February 17, 2005 Fedora Legacy Update Advisory, FLSA:2344, March 7, 2005 **RedHat Security Advisory, RHSA-2005:405-06, April 28, 2005**
PHP Group PHP prior to 5.0.4; Peachtree Linux release 1	Multiple Denial of Service vulnerabilities have been reported in 'getimagesize().' Upgrade available at: http://ca.php.net/get/php-4.3.11.tar.gz/from/a/mirror Ubuntu: http://security.ubuntu.com/ubuntu/pool/main/p/php4/ Slackware: ftp://ftp.slackware.com/pub/slackware/ Debian: http://security.debian.org/pool/updates/main/p/php3/ SUSE: ftp://ftp.SUSE.com/pub/SUSE Gentoo: http://security.gentoo.org/glsa/glsa-200504-15.xml Mandrake: http://www.mandrakesecure.net/en/ftp.php Peachtree: http://peachtree.burdell.org/updates/ **TurboLinux: ftp://ftp.turbolinux.co.jp/pub/TurboLinux/TurboLinux/ia32/** **RedHat: http://rhn.redhat.com/errata/RHSA-2005-405.html** Currently we are not aware of any exploits for these vulnerabilities.	PHP 'getimagesize()' Multiple Denials of Service CAN-2005-0524 CAN-2005-0525	Low	iDEFENSE Security Advisory, March 31, 2005 Ubuntu Security Notice, USN-105-1, April 05, 2005 Slackware Security Advisory, SSA:2005-095-01, April 6, 2005 Debian Security Advisory, DSA 708-1, April 15, 2005 SUSE Security Announcement, SUSE-SA:2005:023, April 15, 2005 Gentoo Linux Security Advisory, GLSA 200504-15, April 18, 2005 Mandriva Linux Security Update Advisory, MDKSA-2005:072, April 19, 2005 Peachtree Linux Security Notice, PLSN-0001, April 21, 2005 **Turbolinux Security Advisory, TLSA-2005-50, April 28, 2005** **RedHat Security Advisory, RHSA-2005:405-06, April 28, 2005**
PHP-Calendar PHP-Calendar 0.x	An SQL injection vulnerability has been reported in 'search.php' due to insufficient sanitization of an unspecified parameter, which could let a remote malicious user execute arbitrary SQL code. Upgrades available at: http://prdownloads.sourceforge.net/php-calendar/php-calendar-0.10.3.tar.gz?download There is no exploit code required.	PHP-Calendar Search.PHP SQL Injection CAN-2005-1397	High	SECUNIA ADVISORY ID: SA15116, April 27, 2005

PHPCart PHPCart 3.x	A vulnerability has been reported in 'phpcart.php' due to insufficient verification of the 'price' and 'postage' parameters, which could let a remote malicious user manipulate invoice and payment charges. No workaround or patch available at time of publishing. A Proof of Concept exploit has been published.	PHPCart Input Validation CAN-2005-1398	Medium	Secunia Advisory, SA15116, April 27, 2005
phpCOIN phpCOIN 1.2, 1.2.1 b, 1.2.1	Multiple SQL injection vulnerabilities have been reported due to insufficient validation of user-supplied input in the 'index.php,' 'login.php,' and 'mod.php' scripts, which could let a remote malicious user execute arbitrary SQL code. No workaround or patch available at time of publishing. There is no exploit code required; however, Proofs of Concepts have been published.	phpCOIN Multiple SQL Injection CAN-2005-1384	High	Dcrab 's Security Advisory, April 28,2005
S9Y Serendipity 0.7, -rc1, beta1-beta4, 0.7.1, Serendipity 0.8 -beta6 Snapshot, 0.8 -beta5 and beta6	Multiple vulnerabilities have been reported: a vulnerability was reported due to insufficient sanitization of unspecified input handled with 'exit.php' and pingbacks before used in an SQL query, which could let a remote malicious user execute arbitrary SQL code; a Cross-Site Scripting vulnerability was reported due to insufficient sanitization of input handled with BBCode before returned to the user, which could let a remote malicious user execute arbitrary HTML and script code; an input validation vulnerability was reported when processing path names for uploaded media, which could let a remote malicious user bypass the validation process; and an input validation vulnerability was reported in the media manager which could let a remote malicious user execute arbitrary code. Upgrades available at: http://www.s9y.org/12.html There is no exploit code required.	Serendipity Multiple Vulnerabilities CAN-2005-1134 CAN-2005-1448 CAN-2005-1449 CAN-2005-1450 CAN-2005-1451 CAN-2005-1452	Medium/ High (High if arbitrary code can be executed)	Secunia Advisory, SA15145, April 27, 2005

[back to top]

Recent Exploit Scripts/Techniques

The table below contains a sample of exploit scripts and "how to" guides identified during this period. The "Workaround or Patch Available" column indicates if vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have published workarounds or patches.

Note: At times, scripts/techniques may contain names or content that may be considered offensive.

Date of Script (Reverse Chronological Order)	Script name	Workaround or Patch Available	Script Description
May 2, 2005	ce_ex.pl ce_ex2.pl ex_ceterm.c	No	Scripts that exploit the ARPUS/Ce Buffer Overflow vulnerability.
May 2, 2005	globalscape_ftp_30_EIP.py globalscape_ftp_30.pm globalscape_ftp_30_SEH.py	Yes	Proofs of Concept exploits for the GlobalSCAPE Secure FTP Server Remote Buffer Overflow vulnerability.
May 2, 2005	MTPBugs.zip	No	Script that exploits the Mtp Target Format String and Denial of Service vulnerability.
April 30,2005	ex_arcgis.c	Yes	Script that exploits the ESRI ArcInfo Workstation Format String vulnerability.
April 29, 2005	filepocket.c	No	Exploit for the FilePocket Local Information Disclosure vulnerability.
April 29, 2005	SNMPPD SNMP Proxy Daemon Remote Format String	No	Script that exploits the SNMPPD SNMP Proxy Daemon Remote Format String vulnerability.
April 27, 2005	altirisClientServicePrivEscalation.c	No	Exploit for the Altiris Deployment Solution AClient Password Protection Bypass vulnerability.
April 27, 2005	nvstatsmngrPrivEsc.c	No	Exploit for the BakBone NetVault NVStatsMngr.EXE Local Privilege Escalation Vulnerability.
April 25, 2005	affixBluetoothIndexPoC.c	No	Proof of Concept exploit for the Affix Bluetooth Protocol Stack Signed Buffer Index vulnerability.

[back to top]

Trends

- **New list of critical vulnerabilities released for Q1 2005:** In an effort to give administrators more timely data to help prioritize patching, the SANS Institute of Bethesda, Md., has begun updating its top 20 list of Internet vulnerabilities on a quarterly basis. The new entries were taken from more than 600 vulnerabilities reported during January, February, and March that affect a large number of users, are unpatched on a substantial number of systems, allow remote exploitation, and have enough information available to make an exploit likely. Source: http://www.gcn.com/vol1_no1/daily-updates/35719-1.html
- **Study shows hackers widening focus**: Online criminals turned their attention to antivirus software and media players in the first three months of

2005 as they sought new ways to take control of users' computers, according to a survey released on Monday, May 1. While hackers continued to poke new holes in Microsoft's Windows operating system, they increasingly exploited flaws in software made by other companies as well, the nonprofit SANS Institute found. "Operating systems have gotten better at finding and fixing things and auto-updating, so it's less fertile territory for the hackers," said SANS Chief Executive Alan Paller. More than 600 new Internet security holes have surfaced in 2005 so far, SANS found. Report: http://www.sans.org/top20/Q1-2005update Source: http://www.reuters.com/newsArticle.jhtml?type=technologyNews&storyID=8359020

- **Online banking needs stronger security:** According to a report from the TowerGroup, advanced approaches to online fraud such as spyware methods, browser hijacking, and remote administration tools post a a significant and fast-growing threat to consumer confidence in the online banking channel. Source: http://www.consumeraffairs.com/news04/2005/online_banking.html
- **Wireless leaders form alliance up to address security:** Cisco and Intel have announced a formal alliance at InfoSec Europe to promote better security for users of wireless networks. They are concerned that fears about security will harm the rollout of wide-scale wireless networks, and have produced advice sheets for businesses, homes and public Wi-Fi access points. Source: http://www.vnunet.com/news/1162761.
- **Hackers attack IT conference**: Security experts that attended the Wireless LAN Event in London found that anonymous hackers in the crowd had created a Web site that looked like a genuine log-in page for a Wi-Fi network, but which actually sent 45 random viruses to computers that accessed it. Source: http://news.zdnet.co.uk/internet/security/0,39020375,39195956,00.htm.

[back to top]

Viruses/Trojans

Top Ten Virus Threats

A list of high threat viruses, as reported to various anti-virus vendors and virus incident reporting organizations, has been ranked and categorized in the table below. For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. It is therefore possible that a virus has infected hundreds of machines but has only been counted once. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages as soon as updates become available. The table lists the viruses by ranking (number of sites affected), common virus name, type of virus code (i.e., boot, file, macro, multi-partite, script), trends (based on number of infections reported since last week), and approximate date first found.

Rank	Common Name	Type of Code	Trends	Date
1	Netsky-P	Win32 Worm	Stable	March 2004
2	Mytob.C	Win32 Worm	Increase	March 2004
3	Zafi-D	Win32 Worm	Stable	December 2004
4	Netsky-Q	Win32 Worm	Decrease	March 2004
5	Zafi-B	Win32 Worm	Increase	June 2004
6	Netsky-B	Win32 Worm	Slight Increase	February 2004
7	Bagle.BJ	Win32 Worm	Decrease	January 2005
8	Netsky-D	Win32 Worm	Decrease	March 2004
9	Bagle-AU	Win32 Worm	Slight Decrease	October 2004
10	Netsky-Z	Win32 Worm	Decrease	April 2004
10	Bagle.BB	Win32 Worm	Return to Table	September 2004
10	Lovgate.w	Win32 Worm	Return to Table	April 2004

Table Updated May 3, 2005

Viruses or Trojans Considered to be a High Level of Threat

- **Cabir**: Cell phone virus cabir, has infected phones across 20 different countries, according to F-Secure the Finnish security company. The virus does not do much harm once it infects a phone besides trying to spread to other devices, but it does have side effects such as draining the battery. Source: http://www.techtree.com/techtree/jsp/showstory.jsp?storyid=3545
- **Sober**: A new variant of the mass-mailing Sober worm has been discovered and is spreading among consumer PC users, security experts said Monday. The messages intend to capitalize on the World Cup and appear in recipients' inboxes as originating from the Fédération Internationale de Football (FIFA). The virus uses a subject header in an e-mail to try to entice people into opening an attachment. The virus then harvests e-mail addresses from the victim and directs a barrage of spam to those addresses. Source: http://www.internetnews.com/security/article.php/3502216

The following table provides, in alphabetical order, a list of new viruses, variations of previously encountered viruses, and Trojans that have been discovered during the period covered by this bulletin. This information has been compiled from the following anti-virus vendors: Sophos, Trend Micro, Symantec, McAfee, Network Associates, Central Command, F-Secure, Kaspersky Labs, MessageLabs, Panda Software, Computer Associates, and The WildList Organization International. Users should keep anti-virus software up to date and should contact their anti-virus vendors to obtain specific information on the Trojans and Trojan variants that anti-virus software detects.

NOTE: At times, viruses and Trojans may contain names or content that may be considered offensive.

Name	Aliases	Type
Agent.aa	Bancos.NL Trojan-PSW.Win32.Agent.aa	Win32 Worm
Appdisabler.A	SymbOS/Appdisabler.A	Symbian OS Worm
Backdoor.Doyorg	Backdoor.Win32.Agent.jn W32/Oscarbot	Win32 Worm
Backdoor.Heplane		Trojan
Backdoor.Lingosky	Backdoor.Win32.Agent.jk	Trojan

Backdoor.Staprew.B	Trojan-Proxy.Win32.Fireby.b	Trojan
BackDoor-CQL	Backdoor.Win32.Vatos	Trojan
BackDoor-CQQ	Troj/Dloader-LI Trojan.Win32.Agent.cp TROJ_AGENT.QW Win32.SillyDl.LR	Trojan
Bancos.NL	Trj/Bancos.NL Trj/Banker.NL	Trojan
Cabir.V	EPOC/Cabir.V SymbOS/Cabir.V Worm.Symbian.Cabir.V	Symbian OS Worm
Cabir.Y	EPOC/Cabir.Y SymbOS/Cabir.Y Worm.Symbian.Cabir.Y	Symbian OS Worm
Email-Worm.Win32.Antiman		Win32 Worm
Kedebe.B	W32/Kedebe.B.worm	Win32 Worm
Nopir.A	W32/Nopir.A.worm	Win32 Worm
PWSteal.Bancos.U		Trojan
Skulls.I	SymbOS/Skulls.I	Symbian OS Worm
Skulls.J	SymbOS/Skulls.J	Symbian OS Worm
Skulls.K	SymbOS/Skulls.K	Symbian OS Worm
SymbOS/Locknut.C		Symbian OS Worm
Troj/Bbprox-A		Trojan
Troj/LegMir-DR	Trojan-PSW.Win32.Lmir.adt PWS-LegMir.dr	Trojan
Troj/PcClient-R	Backdoor.Win32.PcClient.x BackDoor-CKB.dr	Trojan
Troj/Zlob-I	Trojan-Downloader.Win32.Zlob.i	Trojan
Trojan.Riler.D		Trojan
Trojan.StartPage.O		Trojan
Trojan.Vundo.B		Trojan
Uploader-X		Trojan
VBS_BANISH.A		Visual Basic Worm
W32.Allim.A		Win32 Worm
W32.Allim.B	IM-Worm.Win32.Opanki.a	Win32 Worm
W32.Gaobot.DEY	Backdoor.Win32.Rbot.gen	Win32 Worm
W32.Kelvir.AX		Win32 Worm
W32.Kelvir.AZ		Win32 Worm
W32.Kelvir.BA		Win32 Worm
W32.Kelvir.BD	IM-Worm.Win32.Prex.d	Win32 Worm
W32.Mydoom.BL@mm	Email-Worm.Win32.Mydoom.as W32/MyDoom-BN W32/Mydoom.bn@MM WORM_MYDOOM.AQ	Win32 Worm
W32.Mytob.BR@mm		Win32 Worm
W32.Mytob.BS@mm		Win32 Worm
W32.Mytob.BT@mm		Win32 Worm
W32.Netsky.AI@mm		Win32 Worm
W32.Spybot.OFN		Win32 Worm
W32.Spybot.OGX		Win32 Worm
W32.Topion.A		Win32 Worm
W32/Agobot-RV		Win32 Worm
W32/Banish-A	W32.Banish.A@mm WORM_BANISH.A	Win32 Worm
W32/Bropia.worm.aj		Win32 Worm
W32/Icpass-A		Win32 Worm
W32/Kassbot-C	BackDoor-CPV Backdoor.Win32.Delf.yo	Win32 Worm
W32/MyDoom-BN	Email-Worm.Win32.Mydoom.as	Win32 Worm
W32/Mytob-BT		Win32 Worm
W32/Mytob-BW	WORM_MYTOB.BW	Win32 Worm
W32/Rbot-ABO		Win32 Worm
W32/Rbot-ABP		Win32 Worm
W32/Sdbot-XV		Win32 Worm
W32/Sdbot-XW	Backdoor.Win32.Rbot.oq	Win32 Worm

W32/Sober.p@MM	Email-Worm.Win32.Sober.p Sober.P Sober.V W32.Sober.O@mm W32/Sober-N W32/Sober.gen@MM W32/Sober.V.worm Win32.Sober.N Win32Sober.N WORM_SOBER.S	Win32 Worm
W32/Sober-N	Win32.Sober.N	Win32 Worm
Win32.Mydoom.BL		Win32 Worm
WORM_AHKER.H		Win32 Worm
WORM_EZIO.A		Win32 Worm
WORM_FRANCETTE.R		Win32 Worm
WORM_KEDEBE.C		Win32 Worm
WORM_KELVIR.AH	W32/Generic.worm!p2p	Win32 Worm
WORM_KELVIR.AL		Win32 Worm
WORM_KELVIR.AN		Win32 Worm
WORM_MYTOB.DB		Win32 Worm
WORM_MYTOB.DC		Win32 Worm
WORM_MYTOB.DG		Win32 Worm
WORM_MYTOB.DJ		Win32 Worm
WORM_NOPIR.B		Win32 Worm
WORM_OPANKI.A		Win32 Worm
WORM_OPANKI.B		Win32 Worm
WORM_OPANKI.C		Win32 Worm
WORM_SCOLD.C		Win32 Worm

[back to top]

Last updated May 04, 2005